EMMANUEL BRIAND

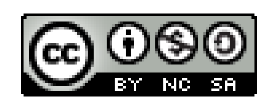
INTRODUCCIÓN A LA MATEMÁTICA DISCRETA

GRADO EN INGENIERÍA INFÓRMATICA

ETSII. UNIVERSIDAD DE SEVILLA

VERSION 1.5
DICIEMBRE DE 2011

http://emmanuel.jean.briand.free.fr/docencia/IMD/Material_IMD/ApuntesIMD_EB/



Creditos: Para elaborar este texto me he insiprado de varias presentaciones existentes, e incluso he copiado ejemplos provenientes de otros textos. Para las partes de aritmética, utilizé así los apuntes de introduciión a la matemática discreta de Javier Cobos Gavala[1].

La parte de combinatoria la derivé de los apuntes de Eric Lehman y Srinivas Devadas [2] para la asignatura *Mathematics for Computer Science* impartida en el M.I.T. Dichos apuntes estan integrados en el *MIT OpenCourseWare*.

Finalmente para el primer cápitulo utilizé material existente elaborado por varios profesores de mi departamento.

[1] Javier Cobis Gavala. Apuntes de introducción a la matemática discreta para la titlación de ingeniería informática. Departamento de matemática Aplicada 1. http://ma1.eii.us.es/Material/IMD_ii_Ap.pdf (consultado el 1ero de diciembre de 2011)

[2] Srinivas Devadas and Eric Lehman. 6.042J/18.062J Mathematics for Computer Science, Spring 2005. Massachussets Institute of Technology: MIT OpenCourseWare. http://ocw.mit.edu (consultado el 1ero de septiembre de 2010). Licencia: Creative Commons BY-NC-SA

Índice general

Bibliografía

Javier Cobis Gavala. Apuntes de introducción a la matemática discreta para la titlación de ingeniería informática. Departamento de matemática Aplicada 1. http://ma1.eii.us.es/Material/IMD_ii_Ap.pdf (consultado el 1ero de diciembre de 2011).

Srinivas Devadas and Eric Lehman. 6.042J/18.062J Mathematics for Computer Science, Spring 2005. Massachussets Institute of Technology: MIT OpenCourseWare. http://ocw.mit.edu (consultado el 1ero de septiembre de 2010). Licencia: Creative Commons BY-NC-SA.

Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: a foundation for computer science*. Addison–Wesley, 1994.

Ralph P. Grimaldi. *Matemáticas discretas y combinatoria: una introducción con aplicaciones*. Addison–Wesley Iberoamericana, 1998.

1

Lógica, Teoría de conjuntos, Álgebras de Boole

Esta parte del curso está dedicada al "lenguaje de la matemática": la lógica proposicional y la teoría de conjuntos.

NOTA BENE.

With each copy of this Book is given an Envelope, containing a Diagram (similar to the frontispiece) on card, and nine Counters, four red and five grey.

The Envelope, &c. can be had separately, at 3*d*. each.

The Author will be very grateful for suggestions, especially from beginners in Logic, of any alterations, or further explanations, that may seem desirable. Letters should be addressed to him at "29, Bedford Street, Covent Garden, London."

1.1 Lógica

1.1.1 Proposiciones

En matemáticas, consideramos frases que son o bien verdaderas (=ciertas), o bien falsas, como las siguientes:

"$2+3=4$"

"Hoy es lunes"

"Si $x=2$ entonces $x^2=4$"

Estas frases las llamamos *proposiciones*. No son proposiciones frases como:

"Ojalá no llueva hoy !"

La frase siguiente,

"$x>0$ y $x<1$."

tampoco es una proposición, cuando x es una variable sin valor asignado, porque puede ser verdadera o falsa, dependiendo del valor de x. Estas frases las llamamos *predicados*.

Nos referimos al carácter "verdadero" o "falso" de una proposición con la palabra *valor de verdad* de la proposición: el valor de verdad de una proposición verdadera es "verdadera", y el valor de verdad de una proposición falsa es "falsa".

Ejemplo 1.1.1.
Considérese:

"Existe una infinidad de números primos p tal que $p+2$ es primo."

No sabemos si esta frase es verdadera o falsa (es un problema sin resolver en matemáticas). Sin embargo, esta frase es bien una proposición. Simplemente, ignoramos su valor de verdad. $\lozenge$

Ejemplo 1.1.2.
Determinar, para cada una de las frases siguientes, si son proposiciones o no. Determinar, cuando se pueden su valor de verdad (*cierta* o *falsa*).

1. "Napoleón ganó la batalla de Austerlitz".
2. "$2+2=5$".
3. "Cierra la puerta".
4. "$x \geq 2$".



1.1.2 *Componiendo proposiciones: y, o, no, implicación, equivalencia*

Considérese la proposición siguiente:

"Hoy es lunes y llueve"

Esta proposición es *compuesta* de dos proposiciones más pequeñas (la primera es "Hoy es lunes", la segunda es "llueve") por medio de un *conector lógico* ("y"). Aquí están otros ejemplos de proposiciones compuestas:

"Si llueve, no salgo"

"$5 \geq 3$ y $5 \leq 6$"

Las proposiciones que no son compuestas, las llamamos *proposiciones simples*, como:

"$5 \geq 3$".

Hay muchos conectores lógicos, pero cinco de ellos son fundamentales. Están presentados en el cuadro 1.1.

! Ojo ¡ El sentido en matemáticas de estas palabras puede diferir del que se les da en el lenguaje ordinario o en filosofía.

A continuación examinamos de más cerca estos cinco conectores lógicos.

El conector "**o**"

A partir de dos proposiciones p, q se forma una nueva proposición: "p **o** q". Su valor de verdad es determinado a partir de los valores de p y de q de la manera siguiente: "p **o** q" es verdadera si por lo menos una de las dos proposiciones p, q es verdadera, y es falsa cuando ambas son falsas.

Por ejemplo,

"$5 > 3$ **o** $5 < 4$"

es verdadera, ya que "$5 > 3$" es verdadera.

Conector	Proposición compuesta	Formas equivalentes	símbolos
y	p **y** q	Conjunción de p y de q.	$p \wedge q$ p && q
o	p **o** q	Disyunción de p y de q.	$p \vee q$ $p \mid\mid q$
no	**no** p	Negación de p.	$\neg p$ $\overline{p}$ $!p$
implica	p **implica** q	**Si** p **entonces** q. Implicación. Condicional. p es una condición suficiente para q. q es una condición necesaria para p.	$p \Rightarrow q$ $p \rightarrow q$
si y solo si	p **si y solo si** q	p **ssi** q. p **es equivalente a** q Bicondicional.	$p \Leftrightarrow q$ $p \leftrightarrow q$

Cuadro 1.1: Los cinco conectores lógicos fundamentales.

Se puede resumir esta definición utilizando una *tabla de verdad*:

p	q	p **o** q
V	V	V
V	F	V
F	V	V
F	F	F

Explicación: hay cuatro posibilidades para los valores de verdad de p y de q, que corresponden a las cuatro filas de la tabla. La segunda fila, por ejemplo, indica que si p es verdadera (V) y q es falsa (F) entonces "p **o** q" es verdadera (V).

Observación: Este "**o**" matemático no es el "o exclusivo" utilizado a menudo en el lenguaje ordinario, como en:

"En este menú, puede pedir un café o un postre."

Interpretación en lenguaje ordinario :	Interpretación en lenguaje matemático :
Puedo pedir o bien el café, o bien el postre, pero no ambos.	Puedo pedir el café, puedo pedir el postre, y puedo también pedir ambos.

Este "o exclusivo" (que corresponde más explícitamente a "o bien . . . o bien . . .) también es un conector lógico (aunque no hace parte de los "cinco fundamentales" presentados aquí). Tiene una tabla de

verdad diferente de la del "**o**":

p	q	p **o (exclusivo)** q
V	V	F
V	F	V
F	V	V
F	F	F

El "o exclusivo" se abrevia a veces en XOR (como "e**x**clusive **or**") en ciertos lenguajes de programación.

El conector "**y**"

Dadas dos proposiciones p y q (por ejemplo, p es "hoy es lunes" y q es "llueve"), definimos una nueva proposición "p **y** q". Le atribuimos un valor de verdad así: "p **y** q" es verdadera si ambas proposiciones son verdaderas, y es falsa sino. O sea, es el "**y**" del lenguaje ordinario.

La tabla de verdad de "**y**" es:

p	q	p **y** q
V	V	V
V	F	F
F	V	F
F	F	F

El conector "**no**".

A partir de una proposición p formamos una nueva proposición: " **no** p". La proposición " **no** p" es verdadera cuando p es falsa, y falsa cuando p es verdadera.

La tabla de verdad de la negación es:

p	**no** p
V	F
F	V

El conector de equivalencia

A partir de dos proposiciones p, q formamos una nueva proposición: "p **es equivalente a** q". Se puede emplear con el mismo sentido: "p **si y solo si** q" (abreviación: "p **ssi** q"). La proposición "p **es equivalente a** q" es verdadera cuando p y q tienen el mismo valor de verdad, y falsa sino:

p	q	p **es equivalente a** q
V	V	V
V	F	F
F	V	F
F	F	V

Ejemplo 1.1.3.

Cuándo resolvemos sistemas de ecuaciones solemos razonar por equivalencia. El sistema es una proposición, que cambiamos por etapas en

sistemas, cada uno obviamente equivalente al anterior (= proposiciones, cada una equivalente al anterior), hasta llegar a una descripción explicita de las soluciones. Consideremos un ejemplo concreto. Queremos resolver:

$$\begin{cases} x & +2y & = 0 \\ 3x & +4y & = 1 \end{cases}$$

Lo que sigue es una resolución bien redactada, con relaciones lógicas explicitas:

Sea $(x, y) \in \mathbb{R}^2$. Entonces

$$\begin{cases} x & +2y & = 0 \\ 3x & +4y & = 1 \end{cases}$$

es equivalente a

$$\begin{cases} x & +2y & = 0 \\ & -2y & = 1 \end{cases}$$

Esta proposición es equivalente a:

$$\begin{cases} x & +2y & = 0 \\ & y & = -1/2 \end{cases}$$

Es equivalente a:

$$\begin{cases} x & -1 & = 0 \\ & y & = -1/2 \end{cases}$$

Es equivalente a:

$$\begin{cases} x & = 1 \\ y & = -1/2 \end{cases}$$

En resumen, tenemos que $\left\{\begin{smallmatrix} x & +2y & =0 \\ 3x & +4y & =1 \end{smallmatrix}\right.$ es equivalente a "$x = 1$ y $y = -1/2$". Por lo tanto el sistema tiene una única solución, es $x = 1, y = -1/2$.

◊

El conector de implicación

A partir de dos proposiciones p y q formamos la nueva proposición "p **implica** q". Se puede emplear con el mismo sentido: "**si** p **entonces** q".

Este conector es el más complicado de los cinco. En efecto, la implicación matemática tiene un sentido bien diferente de la implicación del lenguaje ordinario. El valor de verdad de la implicación p **implica** q se define así: la implicación es falsa solamente cuando la hipótesis p es cierta mientras que la conclusión q es cierta[1]. En todos los otros casos, la implicación es cierta. En particular:

- Si la hipótesis p es falsa, entonces la implicación es cierta, independientemente del valor de q.
- Si la conclusión q es cierta, entonces la implicación es cierta, independientemente del valor de p.

¡ Ojo a este !
Puedes encontrar consideraciones más profundas sobre este conector en el blog de Timothy Gowers (laureato de la medalla Fields – algo como "el premio Nobel de matemáticas"– en 1998): `http://gowers.wordpress.com/2011/09/28/basic-logic-connectives-implies/`

[1] Me gusta pensar así: la implicación es falsa solamente cuando la pillamos *in fraganti* mintiendo.

Aquí esta la tabla de verdad de la implicación:

p	q	p **implica** q
V	V	V
V	F	F
F	V	V
F	F	V

Ejemplo 1.1.4.

- Las proposiciones siguientes son verdaderas:

  "**si** $x = 1$ **entonces** $x + 1 = 2$."
  "$x = 1$ **si y solo si** $x + 1 = 2$."

- En cambio, de las dos proposiciones siguientes:

  "**si** $x = 1$ **entonces** $x^2 = 1$."
  "$x = 1$ **si y solo si** $x^2 = -1$."

  solamente la primera es cierta (la segunda es falsa porque para $x = -1$, se tiene que $x = 1$ es falsa pero $x^2 = 1$ es verdadera).



Diferencias con la implicación del lenguaje ordinario:

En primer lugar, la implicación del lenguaje ordinario sobreentiende una relación de causalidad entre sus dos partes: "si p entonces q" es incorrecto cuando p no es la causa de q. En matemática no es necesaria la existencia de una relación de causalidad. La implicación matemática expresa solamente una coincidencia de los valores de verdad.

Ejemplo 1.1.5.
"**si** hay vida extraterrestre **entonces** $1 + 1 = 2$"

Interpretación en lenguaje ordinario: la implicación no es correcta, ya que la existencia de vida extraterrestre no es causa de que $1 + 1 = 2$.

Interpretación en Lógica Matemática: La implicación es cierta, ya que la conclusión es cierta. No es necesario comprobar el valor de verdad de la hipótesis. ◊

Ejemplo 1.1.6.
"**si** $1 + 1 = 3$ **entonces** todos los estudiantes excepto uno aprobarán la asignatura"

Interpretación en lenguaje ordinario: la implicación no es correcta, ya que la existencia de vida extraterrestre no es causa de que $1 + 1 = 2$.

Interpretación en Lógica Matemática: La implicación es cierta, porque la hipótesis es falsa. No es necesario comprobar el valor de verdad de la conclusión. ◊

Segundo, se utiliza a menudo, en lenguaje ordinario, a"**si** ... **entonces** ...", como una equivalencia lógica[2].

[2] ¡Incluso en las definiciones de los libros de matemáticos, por ejemplo en:

> "Si n es distinto de 1 y no tiene otro divisor que 1 y el mismo, decimos que n es un número primo."

Hay que entender que n es primo si y solo si n es distinto de 1 y no tiene otro divisor que 1 y él mismo. En cambio, siempre se evita tales ambigüedades en los teoremas y en las demostraciones.

Ejemplo 1.1.7.
"Si llueve, te llamo".

Interpretación en lenguaje ordinario: Si llueve, te llamaré, y si no llueve, no te llamaré. O sea: te llamaré si y solo si lloverá. Es una equivalencia, y no una implicación.

Interpretación en lenguaje matemático: Si llueve, te llamo. No me comprometo a nada si no llueve: puedo llamarte, o no.

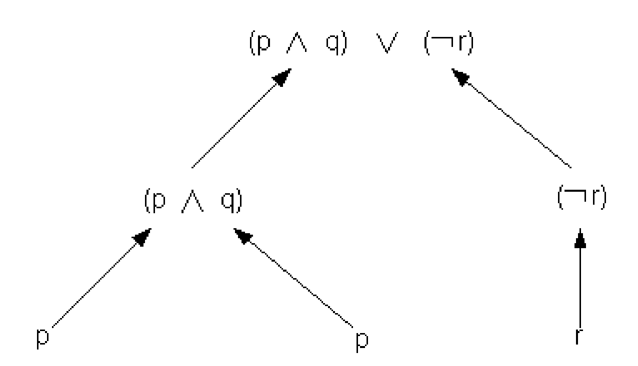
$\Diamond$

Y las paréntesis

Otro elemento que puede aparecer en una proposición son los paréntesis. Estos elementos pueden ser cruciales a la hora de expresar algo. Por ejemplo, no es lo mismo la proposición "$p \vee (q \rightarrow \neg r)$" que "$(p \vee q) \rightarrow \neg r$". La primera se leería "hoy es lunes o si el cielo está despejado entonces hoy hay luna llena", mientras que la segunda sería "si hoy es lunes o el cielo está despejado, entonces hoy hay luna llena".

Señalamos por fin que podemos representar una proposición compuesta, o una formula obtenida a partir de proposiciones indeterminadas (representadas por variables p, q ...), conectores lógicos y paréntesis, por un árbol ("árbol sintético"), en él que partiendo de las proposiciones simples, que se sitúan en la parte inferior del árbol, se van construyendo expresiones más complejas hacia arriba.

Ejemplo 1.1.8.
Aquí está el árbol que representa la formula "$(p \wedge q) \vee (\neg r)$".



$\Diamond$

1.1.3 *Equivalencia lógica de proposiciones*

Consideramos la expresión:

"p **o** ((**no** p) **y** q)"
(o sea, en símbolos: "$p \vee (\neg p \wedge q)$").

donde p y q son proposiciones sin determinar ¿ Cuales son sus posibles valores de verdad en función de los de p y de q ? Podemos contestar por un estudio exhaustivo de los casos, resumido en una tabla de verdad:

p	q	$\neg p$	$\neg p \wedge q$	$p \vee (\neg p \wedge q)$
V	V	F	F	V
V	F	F	F	V
F	V	V	V	V
F	F	V	F	F

y vemos que el valor de verdad de la expresión siempre coincide con el de "p **o** q", independientemente de los valores de verdad de p y de q. Decimos que las expresiones "(p) **o** ((**no** p) **y** q)" y "p **o** q" son *lógicamente equivalentes*.

Definición 1.1.1. Dos expresiones construidas a partir de variables p, q, ... (es decir letras que representan proposiciones sin determinar), conectores lógicos y paréntesis son *lógicamente equivalentes* cuando toman los mismos valores de verdad, para todos los valores de verdad posibles de p y de q.

Ejemplo 1.1.9.
Aquí esta una aplicación del ejemplo anterior en programación. Consideramos la instrucción JAVA siguiente:

```
if (x >0 ||  (x <=0 && y > 100) )
    ...
```

(en JAVA || es el símbolo para " **o** " y && es el símbolo para " **y** ").
Significa:

Si $x > 0$ **o** ($x \leq 0$ **y** $y > 100$)
...

Notamos p para "$x > 0$" y q para "$y > 100$". Observamos que "$x \leq 0$" es lógicamente equivalente a **no** p. Por lo tanto, "$x > 0$ **o** ($x \leq 0$ **y** $y > 100$)" es lógicamente equivalente a "(p) **o** ((**no** p) **y** q)". Por el ejemplo anterior, es lógicamente equivalente a "p **o** q". Por lo tanto, podemos simplificar la instrucción así:

```
if (x >0 || y > 100 )
    ...
```

$\lozenge$

Una equivalencias lógicas importantes

Teorema 1.1.2. *"p **si y solo si** q" es lógicamente equivalente a "(p **implica** q) **y** (q **implica** p)".*

En breve: "$p \Leftrightarrow q$" es lógicamente equivalente a "$(p \Rightarrow q) \wedge (q \Rightarrow p)$".

Las demostraciones de este teorema y de los dos siguientes pueden hacerse mediante tablas de verdad.

Señalamos que la proposición $q \Rightarrow p$ se llama el *recíproco* de la implicación $p \Rightarrow q$. Una proposición y su reciproco no son lógicamente equivalentes, en general. Considerar por ejemplo:

"**si** tengo hambre **entonces** estoy de mal humor."
"**si** estoy de mal humor **entonces** tengo hambre."

Teorema 1.1.3. *"p* **implica** *q" es lógicamente equivalente a "(***no** *p)* **o** *q".*

En breve: "$p \Rightarrow q$" es lógicamente equivalente a $(\neg p) \vee q$.

Teorema 1.1.4. *"p* **implica** *q" es lógicamente equivalente a "(***no** *q)* **implica** *(***no** *p)".*

En breve: "$p \Rightarrow q$" es lógicamente equivalente a "$(\neg q) \Rightarrow (\neg p)$".

La proposición "$(\neg q) \Rightarrow (\neg p)$", lógicamente equivalente a "$p \Rightarrow q$", es llamada el *contrarrecíproco* de "$p \Rightarrow q$". Por lo tanto, cualquiera proposición es lógicamente equivalente a su contrarrecíproco.

Ejemplo 1.1.10.
Para demostrar una proposición, a veces es más fácil demostrar su contrarreciproco. Consideremos m y n dos enteros, y la implicación: "si $m + n$ es par entonces m y n tienen la misma paridad". Para demostrarla, basta demostrar su contrarreciproco, ya que sabemos que la implicación tienen el mismo valor de verdad que su contrarreciproco. El contrarreciproco es: "Si m y n no tienen la misma paridad entonces $m + n$ es impar".

Dos números enteros tienen la misma paridad cuando son o bien ambos pares o bien ambos impares.

> Supongamos, por lo tanto, que m y n no tienen la misma paridad. Uno es par y se puede escribir como $2\,i$ para algún entero i, y el otro es impar y se escribe $2\,j + 1$ para algún entero j. Su suma $m + n$ es igual a $2\,(i + j) + 1$, que es impar.

Esto demuestra bien el contrarreciproco de la implicación inicial, y por lo tanto demuestra también la implicación original. ♢

Señalamos la siguiente notación por si a caso los estudiantes la encuentran: la equivalencia lógica se denota a veces con $\equiv$. Por ejemplo:

$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$$

Damos también la significación de algunas palabras importantes:

- "Contradicción": Una formula es una contradicción si es falsa para toda asignación de los valores de verdad de sus variables. Por ejemplo, $p \Leftrightarrow \neg p$" es una contradicción: es falsa cuando p es verdadero, y falsa también cuando p es falso.

- "Tautología": Una formula es una tautología si es verdadera para toda asignación de los valores de verdad de sus variables. Por ejemplo, $(p \wedge (p \Rightarrow q)) \Rightarrow q$ es una tautología.

En los textos matemáticos se destacan ciertas proposiciones lógicas demostradas, dándoles el nombre de *Teorema*, *Proposición* (en un sentido diferente del de *proposición lógica* visto hasta ahora), de *lema* o de *corolario*. Un *teorema* es un resultado importante del texto; una *proposición* también, pero de importancia algo menor. Un *lema* es un resultado que será utilizado en la demostración de algún teorema o proposición. Un *corolario* es una consecuencia fácil de un teorema o proposición.

1.1.4 *Cálculo de proposiciones*

La expresión:

$\neg((\neg((p \vee q) \wedge r)) \wedge (\neg q))$

puede simplificarse en la expresión mucho más sencilla "$q \vee r$". Se puede demostrar como anteriormente utilizando tablas de verdad. Otra manera de hacer esta simplificación consiste en aplicar ciertas reglas de simplificación. Damos en el cuadro 1.2 una serie de reglas de simplificación (no se pide al estudiante aprenderlas de memoria).

Ejemplo 1.1.11.
Veamos como simplificar la expresión "$\neg((\neg((p \vee q) \wedge r)) \vee (\neg q))$" utilizando estas reglas:

$\neg(\neg((p \vee q) \wedge r) \vee \neg q)$	**Justificación**
$\equiv \neg(\neg((p \vee q) \wedge r)) \wedge \neg(\neg q)$	Ley de De Morgan
$\equiv ((p \vee q) \wedge r) \wedge \neg(\neg q)$	Ley de la doble negación
$\equiv ((p \vee q) \wedge r) \wedge q$	Ley de la doble negación
$\equiv (p \vee q) \wedge (r \wedge q)$	Asociatividad de $\wedge$
$\equiv (p \vee q) \wedge (q \wedge r)$	Conmutatividad de $\wedge$
$\equiv ((p \vee q) \wedge q) \wedge r$	Asociatividad de $\wedge$
$\equiv q \wedge r$	Ley de absorción de $\wedge$

$\Diamond$

$\overline{\overline{p}} \equiv p$	Ley de la doble negación
$\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$ $\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$	Leyes de De Morgan
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Conmutatividad de $\vee$ y $\wedge$
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Asociatividad de $\vee$ y $\wedge$
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributividad de cada una de las operaciones con respecto a la otra
$p \vee p \equiv p$ $p \wedge p \equiv p$	Leyes de idempotencia
$p \vee f \equiv p$ $p \wedge v \equiv p$	v y f son *neutros* para $\wedge$ y $\vee$ respectivamente.
$p \vee v \equiv v$ $p \wedge f \equiv f$	Leyes de dominación
$p \vee \overline{p} \equiv v$ $p \wedge \overline{p} \equiv f$	Leyes de los inversos
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Leyes de absorción

Cuadro 1.2: Las leyes de la lógica proposicional. Aquí v es una tautología (cualquiera), y f es una contradicción (cualquiera). Esta tabla esta dada a título indicativo. No se pide memorizar la lista, ni los nombres. En cambio, tiene que ser capaz de demostrar cada una de estas leyes, y de utilizarlas, con la ayuda del cuadro, como en el ejemplo 1.1.11.

1.2 *Conjuntos*

1.2.1 *Definiciones básicas*

En matemática, un *conjunto* es una colección bien definida de objetos distintos.

Por ejemplo, podemos definir el conjunto de los números 2,4,6 y 8, e identificarlo con la letra A. En símbolos, se escribe:

$$A = \{2, 4, 6, 8\}$$

Las llaves ("$\{$" y "$\}$") son los símbolos reservados para la definición de un conjunto.

Los objetos que forman un conjunto se llaman los *elementos* del conjunto. Se dice de ellos que *pertenecen al conjunto*. Que un objeto x pertenezca a (=sea elemento de) un conjunto C se nota $x \in C$, y que no pertenezca a C se nota $x \notin C$.

En el ejemplo anterior, $2 \in A$ (2 es un elemento de A, pertenece a A) pero $3 \notin A$ (3 no pertenece a A).

Hay que hacer bien la distinción entre un conjunto y sus elementos. Por ejemplo, 1 (número) es distinto de $\{1\}$ (conjunto). Especialmente, no tiene sentido "$2 \in 1$". En cambio "$2 \in \{1\}$" es una proposición bien formada (y falsa).

Ejemplo 1.2.1.

$\{(1,2),(3,2),(1,1)\}$	un conjunto de pares de números
$\{x, y, z\}$	un conjunto de variables
$\{\exp, \cos\}$	un conjunto de funciones
$\{\{1\},\{1,2\},\{2,5\}\}$	un conjunto de conjuntos
$\{1, \exp, \{1\}, \{1,2\}\}$	un conjunto de varios tipos de objetos.

$\lozenge$

Conjunto y orden o repetición de los elementos

La definición de un conjunto no toma en cuenta ningún orden de sus elementos. El conjunto A del ejemplo anterior pude igualmente definirse como $\{2, 6, 4, 8\}$, o $\{8, 6, 4, 2\}$, o ... Las colecciones ordenadas de objetos se llaman *sucesiones* y se suelen notar con paréntesis, como por ejemplo $(2, 4, 6, 8)$ (una sucesión con cuatro términos), o $(2, 6, 4, 8)$ (una sucesión distinta de la anterior).

Observar que, por definición, un conjunto tiene sus elementos distintos, por lo cual es incorrecto escribir $\{2, 4, 2\}$. En cambio, una sucesión puede tener elementos repetidos: $(2, 4, 2)$ es una sucesión bien definida.

Conjuntos finitos y conjuntos infinitos

Un conjunto puede ser *finito* o *infinito*. El número de elementos de un conjunto finito se llama su *cardinal*, y se nota con doble barra $|\quad|$ o con #. Por ejemplo, si $A = \{2, 4, 6, 8\}$ entonces $|A| = 4$ ("A tiene cuatro elementos" o "A tiene cardinal cuatro") . Se puede notar también $\#A = 4$.

símbolo	**conjunto**	**elementos**
$\mathbb{N}$	enteros naturales	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	enteros	$\{\ldots, -2, -1, 0, 1, 2, \ldots$
$\mathbb{Q}$	números racionales	$\frac{1}{2}, -\frac{10}{3}, 1 \ldots$
$\mathbb{R}$	números reales	$\sqrt{2}, \pi, \frac{1}{2}, 1 \ldots$
$\mathbb{C}$	números complejos	$i, \frac{1+i}{2}, \sqrt{2}, \frac{1}{2}, 1, \ldots$

Cuadro 1.3: ciertos conjuntos infinitos importantes se identifican con símbolos reservados.

Definir un conjunto por una propiedad característica de sus elementos

En vez de definir un conjunto dando la lista explicita de sus elementos, se puede definir dando una propiedad característica de sus elementos. Por ejemplo:

> Sea B el conjunto de todos los números enteros pares n que cumplen $n \geq 2$ y $n < 9$.

Esta definición se escribe con símbolos de la manera siguiente:

$$B = \{n \mid \ n \text{ es un entero y } n \geq 2 \text{ y } n < 9\}$$

Explicación:

- Las llaves "$\{$" y "$\}$" indican que se va a definir un conjunto.
- "$\{n \mid \ \ldots\}$" se lee "el conjunto de los n tal que ..." y a continuación se da la propiedad característica de los elementos del conjunto.

Mencionar que la letra n no juega ningún papel particular, y se puede igualmente definir B como, por ejemplo:

$$B = \{w \mid \ w \text{ es un entero y } w \geq 2 \text{ y } w < 9\}$$

¡ Entender estos ejemplos es un ejercicio !

Ejemplo 1.2.2.
Tenemos:

- $[0, +\infty) = \{x^2 \mid x \in \mathbb{R}\}$.
- $\{x \in \mathbb{R} \mid x \geq 0 \text{ y } x^2 \leq x\} = [0, 1]$.
- Dar una descripción más simple de $\{x \in \mathbb{R} \mid x^2 = x\}$

◊

El conjunto vacío

El conjunto más pequeño de todos es $\{\quad\}$, el *conjunto vacío*. Es el conjunto sin ningún elemento. Se suele notar con $\emptyset$. Su cardinal es 0. Tiene muchas descripciones: para una propiedad dada que nunca se da, es el conjunto de los elementos que cumplen esta propiedad. Por ejemplo:

$$\emptyset = \{x \mid x \in \mathbb{N} \text{ y } x + 1 = x\}, \qquad \emptyset = \{x \mid 0 = 1\}.$$

Producto cartesiano de dos conjuntos

Definicion 1.2.1. *Dados dos conjuntos A y B, el conjunto de todos los pares ordenados (a, b) donde a está en A y b en B se denomina producto cartesiano de A por B, y se nota $A \times B$.*

Ejemplo 1.2.3.
Si $A = \{1, 2, 3\}$ y $B = \{a, e\}$, entonces el producto cartesiano $A \times B = \{(1, a), (1, e), (2, a), (2, e), (3, a), (3, e)\}$. Podemos representarlo mediante una tabla:

	1	2	3
a	(1,a)	(2,a)	(3,a)
e	(1,e)	(2,e)	(3,e)

Esto nos deja ver claramente que, si los conjuntos A y B son finitos, entonces $|A \times B| = |A| \cdot |B|$ (el cardinal del producto cartesiano es el producto de los cardinales). ♢

Ejemplo 1.2.4.
El conjunto $\mathbb{R} \times \mathbb{R}$ (también notado $\mathbb{R}^2$) es el conjunto de todos los pares ordenados de números reales: los (x, y), que podemos identificar a los puntos del plano. ♢

1.2.2 *Subconjuntos*

Dados dos conjuntos A y B, se dice que A es un *subconjunto* de B si todo elemento de A es también elemento de B. Se nota $A \subset B$ cuando A es un subconjunto de B (la notación debe evocar "A es más pequeño que B"), y $A \not\subset B$ cuando no lo es.

Ejemplo 1.2.5.

- $\{1,2\} \subset \{1,2,3\}$ pero $\{1,4\} \not\subset \{1,2,3\}$ ya que $4 \notin \{1,2,3\}$.
- $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- $\emptyset \subset \{1,2\}$. De hecho, $\emptyset$ es un subconjunto de todos los conjuntos.

♢

Ejemplo 1.2.6.
Los subconjuntos de $\{1,2\}$ son: $\emptyset$, $\{1\}$, $\{2\}$ y $\{1,2\}$. Es muy importante darse cuenta que 1 **no es** un subconjunto de $\{1,2\}$. El objeto 1 es un número, no es un conjunto. Las proposiciones siguientes son ciertas: $1 \in \{1,2\}$, $1 \in \{1\}$, $\{1\} \subset \{1,2\}$. Las proposiciones siguientes son falsas: $\{1\} \in \{1,2\}$, $1 \subset \{1,2\}$. ♢

Para decir que A es un subconjunto de B, se dice también que A es *una parte* de B, que A *esta contenido en* B, que A esta incluido en B, o que B *contiene* A.

1.2.3 *Operaciones con conjuntos: unión, intersección, diferencia*

Consideramos como ejemplo para las definiciones que siguen $X = \{1,2,3\}$ e $Y = \{1,3,5,7\}$.

- La *unión* $A \cup B$ de dos conjuntos A y B es el conjunto de los objetos que pertenecen a (por lo menos) uno de los dos conjuntos. Ejemplo: $X \cup Y = \{1,2,3,5,7\}$.
- La *intersección* $A \cap B$ de dos conjuntos A y B es el conjunto de los objetos que pertenecen a sendos conjuntos A e B. Ejemplo: $X \cap Y = \{1,3\}$.

- La *diferencia* $A \setminus B$ ("A menos B") es el conjunto de los objetos que pertenecen a A pero no a B. Ejemplo: $X \setminus Y = \{2\}$, $Y \setminus X = \{5,7\}$. Se nota también a veces $A - B$

Representamos convenientemente la unión, la intersección, la diferencia de dos conjuntos, al igual que otras operaciones, mediante diagramas como los de la figura 1.1.

Cuando B es un subconjunto de A, entonces la diferencia $A \setminus B$ se llama también *complementario de A en B*. A menudo, el conjunto A es fijado sin ambigüedad. En este caso el complementario de B en A se nota $\overline{B}$.

Se define igualmente la unión de una colección cualquiera de conjuntos: el conjunto de los objetos que pertenecen a por lo menos uno de los conjuntos. Y la intersección de una colección cualquiera de conjuntos: el conjunto de los objetos que pertenecen a todos los conjuntos de la colección.

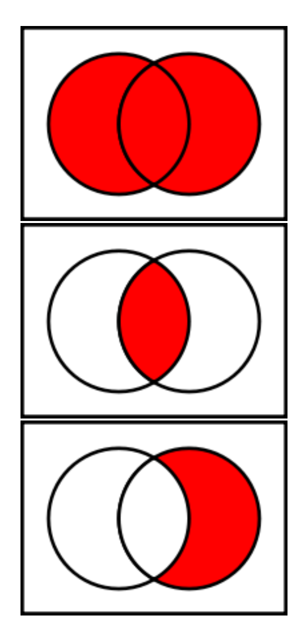


Figura 1.1: Diagramas de conjuntos ("diagramas de Venn"). Los dos discos representan dos conjuntos. En rojo: su unión en el primer diagrama, su intersección en el segundo, y la diferencia (conjunto de la derecha menos conjunto de la izquierda) en el ultimo.

Ejemplo 1.2.7.
Consideramos los conjuntos $[0, 1/n]$ para todos los enteros positivos n. Los conjuntos de esta colección son los intervalos $[0, 1]$ (el conjunto asociado a $n = 1$), $[0, 1/2]$ (asociado a $n = 2$), $[0, 1/3]$ (asociado a $n = 3$) ... La intersección de esta colección infinita de conjuntos es $\{0\}$. $\Diamond$

Se dice de dos conjuntos A y B son *disjuntos* si su intersección es vacía ($A \cap B = \emptyset$).

Ejemplo 1.2.8.
Los intervalos $(-\infty; 0]$ y $[0, +\infty)$ no son disjuntos, ya que su intersección es $\{0\}$. Los intervalos abiertos $(-\infty; 0)$ y $(0, +\infty)$ son disjuntos. Los intervalos $(-\infty; 0]$ y $(0, +\infty)$ también son disjuntos. $\Diamond$

Sabemos que la adición y las multiplicación de los números son "conmutativas" ($a + b = b + a$, $a \times b = b \times a$), "asociativas" ($(a + b) + c = (a + (b + c))$ y similarmente para $\times$, pero al contrario de la división, por ejemplo), que la multiplicación es distributiva con respecto a la adición ($a \times (b + c) = (a \times b) + (a \times c)$). Podemos, de manera similar, hacer una lista de propiedades de las operaciones $\cup$, $\cap$ y complementario sobre los subconjuntos de un conjunto fijo X: ver el cuadro 1.4

Todas estas reglas pueden ser utilizadas en un "cálculo de conjuntos", por ejemplo para simplificar formulas.

Es interesante observar que la unión y la intersección son operaciones sobre conjuntos, como la adición es una operación sobre números. Por ejemplo, podemos construir las tablas de unión y de intersección para los subconjuntos de $\{1, 2\}$:

$\cup$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\{1\}$	$\{1,2\}$	$\{1,2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\{2\}$	$\{1,2\}$
$\{1,2\}$	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$

$\cap$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$	$\{1\}$
$\{2\}$	$\emptyset$	$\emptyset$	$\{2\}$	$\{2\}$
$\{1,2\}$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$

Ejemplo 1.2.9.
Consideramos un conjunto X y los subconjuntos A, B y C de X. Vamos a simplificar la expresión $\overline{\overline{(A \cup B)} \cap C \cup \overline{B}}$, utilizando las reglas del cuadro 1.4.

$\overline{\overline{A}} = A$	Ley del doble complemento
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	Leyes de De Morgan
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Conmutatividad de $\cup$ y $\cap$
$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	Asociatividad de $\cup$ y $\cap$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributividad de cada una de las operaciones con respecto a la otra
$A \cup A = A$ $A \cap A = A$	A es idempotente para ambas operaciones
$A \cup \varnothing = A$ $A \cap X = A$	X y $\varnothing$ son *neutros* para $\cap$ y $\cup$ respectivamente.
$A \cup X = X$ $A \cap \varnothing = \varnothing$	X y $\varnothing$ son *absorbentes* para $\cup$ y $\cap$ respectivamente.
$A \cup \overline{A} = X$ $A \cap \overline{A} = \varnothing$	$\overline{A}$ es inversa de A para $\cup$ y $\cap$
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Leyes de absorción

Cuadro 1.4: Las leyes de la teoría de conjuntos. Aquí X es un conjunto y A, B, C son subconjuntos de X. El estudiante debería ser por lo menos capaz de convencerse de la validez de cada una por medio de diagramas de Venn.

$\overline{\overline{(A \cup B) \cap C} \cup \overline{B}}$	**Justificación**
$= \overline{\overline{(A \cup B) \cap C}} \cap \overline{\overline{B}}$	Ley de De Morgan
$= ((A \cup B) \cap C) \cap \overline{\overline{B}}$	Ley del doble complemento
$= ((A \cup B) \cap C) \cap B$	Ley del doble complemento
$= (A \cup B) \cap (C \cap B)$	Asociatividad de $\cap$
$= (A \cup B) \cap (B \cap C)$	Conmutatividad de $\cap$
$= ((A \cup B) \cap B) \cap C$	Asociatividad de $\cap$
$= B \cap C$	Ley de absorción de $\cap$

$\Diamond$

Finalmente, vamos a dar una demostración formal de unas de estas reglas, como ejemplo de demostración.

Demostramos que para cualesquier subconjuntos A y B de un conjunto X, se tiene $\overline{A \cup B} = \overline{A} \cap \overline{B}$ (una de las leyes de De Morgan).

Demostración. Sea $x \in X$. Por definición del complementario, "$x \in \overline{A \cup B}$" es equivalente a "$x \notin A \cup B$". Es la negación de: "$x$ pertenece a A o a B". Por lo tanto, es equivalente a "x no pertenece ni a A ni a B", que es equivalente a "$x \in \overline{A} \cap \overline{B}$". Esto establece que $x \in \overline{A \cup B}$ si y solo si $x \in \overline{A} \cap \overline{B}$. Los dos conjuntos tienen los mismos elementos, por lo tanto son iguales. $\square$

Demostramos que para cualesquier conjuntos A, B y C, se tiene $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributividad de $\cap$ con respecto a $\cup$).

Demostración. Vamos a demostrar en primero que $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$, y luego que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. O sea: que todo elemento del primer conjunto es elemento del segunda, y *vice–versa*. Esto demostrará bien que los dos conjuntos tienen los mismos elementos, o sea: que son iguales. (Este tipo de demostración de la igualdad de dos conjuntos de llama "demostración de la doble–inclusión").

Demostremos $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Sea $x \in A \cap (B \cup C)$. En particular $x \in A$, y $x \in B \cup C$. Por lo tanto $x \in B$ o $x \in C$. En el primer caso ($x \in B$), obtenemos $x \in A \cap B$. En el segundo caso ($x \in C$), obtenemos $x \in A \cap C$. En ambos casos podemos concluir que $x \in (A \cap B) \cup (A \cap C)$. Esta así demostrada la inclusión anunciada. En efecto, hemos comprobado que todo elemento x de $A \cap (B \cup C)$ pertenece también a $(A \cap B) \cup (A \cap C)$.

Demostremos ahora que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Sea $x \in (A \cap B) \cup (A \cap C)$. Otra vez examinamos los dos casos posibles: $x \in (A \cap B)$ o $x \in (A \cap C)$. En el primer caso tenemos $x \in A$. Tenemos también $x \in B$ y por lo tanto $x \in (B \cup C)$. Concluimos que $x \in A \cap (B \cup C)$. El segundo caso se trata de la misma manera, intercambiando los papeles de B y C. En ambos casos, $x \in A \cap (B \cup C)$. esto demuestra la inclusión anunciada, y acaba la demostración de la igualdad de los conjuntos. $\square$

1.3 *Álgebras de Boole*

El álgebra de conjuntos y el álgebra de proposiciones presentan grandes paralelismos. Hay un concepto matemático que generaliza ambas teorías, y otras: el concepto de *álgebra de Boole*.

Definicion 1.3.1. *Un álgebra de Boole es un conjunto B con:*

- *dos operaciones, que se suelen llamar* suma *y* producto *y notar con* $+$ *y* $\times$ *(o, a veces, por solamente un punto:* $\cdot$*),*
- *una transformación que asocia a cada elemento de x un elemento x' de B que se suele llamar complementario*
- *elementos distinguidos* 0 *y* 1

tal que todas las leyes del cuadro 1.5 se verifican.

$(x')' = x$	Ley del doble complementario
$(x+y)' = x' \times y'$ $(x \times y)' = x' + y'$	Leyes de De Morgan
$x+y = y+x$ $x \times y = y \times x$	conmutatividad de $+$ y $\times$
$(x+y)+z = x+(y+z)$ $(x \times y) \times z = x \times (y \times z)$	asociatividad de $+$ y $\times$
$x \times (y+z) = (x \times y) + (x \times z)$ $x + (y \times z) = (x+y) \times (x+z)$	Distributividad de cada una de las operaciones con respecto a la otra
$x+x = x$ $x \times x = x$	Cada x es idempotente para ambas operaciones
$x+0 = x$ $x \times 1 = x$	1 y 0 son *neutros* para $\times$ y $+$ respectivamente.
$x+1 = 1$ $x \times 0 = 0$	Leyes de dominación
$x+x' = 1$ $x \times x' = 0$	Leyes de los inversos
$x+(x \times y) = x$ $x \times (x+y) = x$	Leyes de absorción

Cuadro 1.5: Las leyes de las álgebras de Boole

Ejemplos fundamentales:

- Sea X un conjunto. Entonces el conjunto de todos los subconjuntos de X, con $\cup$ y $\cap$ para las operaciones $+$ y $\times$, y $A' = \overline{A}$ para el complementario, es un álgebra de Boole.

- El conjunto $\{V, F\}$ (conjunto de los dos valores de verdad) es un álgebra de Boole, con $\wedge$ y $\vee$ como operaciones $+$ y $\times$, y $p' = \neg p$ para el complementario, es un álgebra de Boole.

El teorema siguiente nos dice que para comprobar que un conjunto B con operaciones $+$, $\times$ y $'$ es un álgebra de Boole, nos tenemos que comprobar todas las propiedades de la definición, sino solamente unas pocas.

Teorema 1.3.2. *Sea B un conjunto con operaciones $+$, $\times$ y $'$ y elementos* 0 *y* 1. *Si cumple las leyes:*

- *conmutatividad de $+$ y $\times$.*
- *asociatividad de $+$ y $\times$.*
- *Distributividad de cada una de las operaciones$+$ y $\times$ con respecto a la otra.*
- 1 *y* 0 *son* neutros *para $\times$ y $+$ respectivamente.*
- *Leyes de los inversos.*

entonces necesariamente cumple también las otras leyes, y B es un álgebra de Boole.

Ejemplo 1.3.1.
Como ilustración, enseñamos la demostración abstracta de la ley de dominación $x + 1 = x$ directamente a partir de las conco propiedades del teorema.

$$\begin{aligned} x+1 &= 1 \times (x+1) && \text{porque 1 es neutro para } \times. \\ &= (x+x') \times (x+1) && \text{por les leyes de los inversos.} \\ &= x + (x' \times 1) && \text{por distributividad.} \\ &= x + x' && \text{porque 1 es neutro para } \times. \\ &= 1 && \text{por las leyes de los inversos.} \end{aligned}$$

◊

Otro ejemplo: circuitos de conmutación

En otra asignatura los estudiantes encontrarán un ejemplo más de álgebras de Boole: la *álgebra de conmutación* del análisis de circuitos electrónicos. Se consideran *circuitos de conmutación* como él de la figura 1.2.

La asignatura *Circuitos electrónicos digitales*. Los estudiantes harán *muchos* ejercicios con circuitos de conmutación.

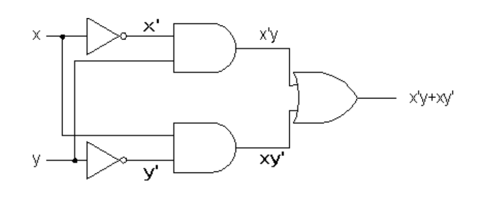


Figura 1.2: Un circuito de conmutación.

Un circuito de conmutación consiste en un *conjunto de entradas*, un *procesador* y un *conjunto de salidas*. Las entradas y las salidas se suelen representar gráficamente como segmentos. Son variables que toman los posibles valores binarios, en función de si están activas o no: cuando circula corriente a través de ellas toman el valor 1; en caso contrario toman el valor 0. Esto hace que los circuitos sean considerados sistemas binarios. El procesador se compone de distintos componentes simples que se pueden combinar entre sí y a los que se denomina *puertas*. Fundamentalmente se utilizan tres puertas: *AND*,

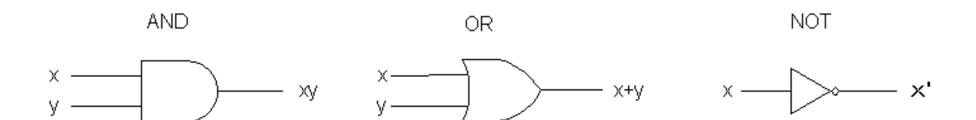


Figura 1.3: Las puertas lógicas AND, OR y NOT.

OR, *NOT*. Gráficamente se representan mediante distintos símbolos, aunque quizás los más usuales son los siguientes.

El *álgebra de conmutación* es el álgebra de Boole cuyo conjunto es $\{0,1\}$ y cuyas operaciones $+$, $\times$ y complementario son definidas por las tablas:

$+$	0	1
0	0	1
1	1	1

$\times$	0	1
0	0	0
1	0	1

x	x'
0	1
1	0

Es fácil comprobar que se trata de una reescritura de álgebra de Boole de la lógica proposicional, tomando $F = 0$, $V = 1$, $+ = \vee$, $\times = \wedge$, $' = \neg$.

Las operaciones son realizadas por las puertas:

- La puerta AND actúa sobre dos variables binarias x, y mediante la operación $\times$, de manera que las entradas son las dos variables x, y y la salida es xy.
- La puerta OR actúa sobre dos variables binarias x, y mediante la operación $+$, siendo las entradas las dos variables x, y y la salida el valor correspondiente a $x + y$.
- La puerta NOT actúa sobre una variable x mediante la operación $'$, de forma que la entrada es la variable x y la salida es x'.

Ejemplo 1.3.2.
El circuito de la figura 1.2 representa la función de conmutación $x'y + xy'$. ♢

Ejemplo 1.3.3.
El circuito de la figura 1.4 produce la función de conmutación $xy + z'$: ♢

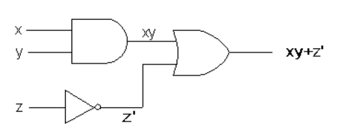
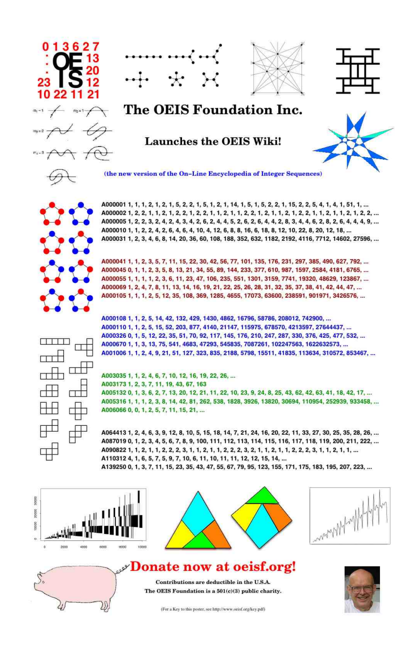


Figura 1.4: El circuito con función de conmutación $xy + z'$.

2
Combinatoria

2.1 Contar

En esta parte del curso presentamos una variedad de reglas y principios para contar: dado un conjunto finito, ¿ Podemos contar sus elementos (sin hacer la lista de dichos elementos, claro está) ?



Ejemplo 2.1.1. Un problema de reparto, y el truco de colocar $k-1$ barras entre n objetos para forma k grupos.

- **Pregunta 1:** Si cinco niños comparten 12 canicas idénticas ¿ De cuantas maneras pueden repartírselas ? (Por ejemplo: 2 para el primer niño, 2 para el segundo, ninguna para el tercero, 5 para el cuarto y 3 para el último)
- **Pregunta 2:** ¿ Cuántos números de 16 bits tienen *exactamente* cuatro "1" ? (Por ejemplo 0010011000001000.)

Sorprendentemente, las dos preguntas tienen la misma respuesta. En efecto, dibujemos las 12 canicas:

oooooooooooo

La distribución de las canicas con 2 canicas para el primer niño, 2 para el segundo, ninguna para el tercero, 5 para el cuarto y 3 para el último, la representamos así:

oo/oo//ooooo/ooo

Es decir, formamos los grupos de canicas que atribuimos a los niños, introduciendo separaciones. Como son 5 niños, hace falta 4 separaciones. Así, las posibles distribuciones de las canicas corresponden a todas las posibles sucesiones de 12 símbolos "o" y 4 símbolos "/". En total, son 16 símbolos. En fin, el número de posibles distribuciones es el número de posibles elecciones de las posiciones de los 4 símbolos "/" entre las 16 posiciones posibles. Cambiando los "o" en "0" (cero) y los "/" en "1" vemos que se trata exactamente del problema de la pregunta 2. ♢

¿ Por qué contar ?

Contar es útil en informática por varias razones. Entre otras:

- Determinar el tiempo y la memoria necesarios para la resolución de un problema de cálculo se reduce a menudo a un problema de contar.
- Contar es la base de las probabilidades.

2.2 *El principio de la biyección*

El principio de biyección dice que, si podemos poner dos conjuntos "en correspondencia", entonces tienen el mismo número de elementos. Nos hace falta decir más precisamente lo que significa "poner dos conjuntos en correspondencia" (diremos : establecer una biyección entre los dos conjuntos). Para esto, necesitamos introducir las nociones de *aplicación* y de *biyección*.

2.2.1 *Aplicaciones*

Damos en primer lugar una definición simple, pero algo incompleta, de *aplicación*.

"Función" casi es sinónimo de "aplicación".

Definicion 2.2.1. *Sean A y B dos conjuntos. Definimos una* aplicación de A en B *asociando a cada elemento de A un elemento de B.*

La definición 2.2.1 carece de precisión. Hay una definición moderna muy precisa, pero menos directa. El *grafo* de una aplicación es el conjunto de todos los pares $(a, f(a))$ con $a \in A$. Si G es un subconjunto del producto cartesiano $A \times B$ (es decir: un conjunto de pares (a, b) con $a \in A$, $b \in B$) es el grafo de una aplicación si y solo si para cada $x \in A$ hay un único par $(a, b) \in G$ tal que $a = x$. La definición moderna de *aplicación* es: el dato de los dos conjuntos A y B y de un subconjunto G de $A \times B$ que es un grafo de aplicación de A en B.

Ejemplo 2.2.1.
Definamos una aplicación f de $\mathbb{Z}$ en $\mathbb{Z}$ de la manera siguiente: asociamos a cada entero n par el entero $n/2$ y a cada entero n impar el entero $(n-1)/2$.

En formulas: para cualquier $n \in \mathbb{Z}$

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ es par} \\ (n-1)/2 & \text{si } n \text{ es impar} \end{cases}$$

Cada aplicación admite varias descripciones. La aplicación f también es la aplicación de $\mathbb{Z}$ en $\mathbb{Z}$ que asocia a cada entero n el mayor entero k de los que cumplen $2k \leq n$. ◊

Ejemplo 2.2.2.
Sea $X = \{1, 2, 3\}$ e $Y = \{a, b, c, d\}$. Definamos una aplicación g de X en Y asociando d a 1 y a 2, y c a 3. Se puede resumir esta definición de g por una tabla, como sigue, o un diagrama (figura 2.1).

x	1	2	3
$g(x)$	d	d	c

◊

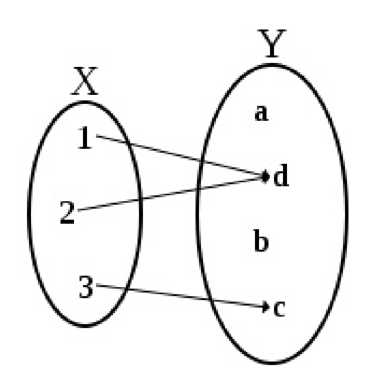


Figura 2.1: Ejemplo 2.2.2.

Si f es una aplicación de A en B entonces:

- A se llama el *conjunto de partida* de f (también su *dominio*).
- B se llama el *conjunto de llegada* de f.
- Para $a \in A$, el único elemento b de B que le corresponde por f se llama *imagen de a por f*. Se nota $b = f(a)$.

- Para $b \in B$, los elementos $a \in A$ que le corresponden por f (es decir: tal que $f(a) = b$) se llaman los *antecedentes de* b. El conjunto de los antecedentes de b es *la fibra de* f *encima de* b.

La notación $f : A \to B$ significa: "f es una aplicación de A en B". Si f es definida por una regla se puede notar:

$$\begin{array}{rccc} f: & A & \to & B \\ & a & \mapsto & \text{descripción de la regla} \end{array}$$

Ejemplo 2.2.3.
Por ejemplo para definir la función f de los enteros en los enteros que cumple $f(n) = \frac{n(n+1)}{2}$ se puede notar:

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & \frac{n(n+1)}{2} \end{array}$$

◊

Ejemplo 2.2.4.
Hay a aplicación f de $\mathbb{R}$ en $\mathbb{R}$ definida por $f(x) = \exp(x)$ (la función exponencial), y otra aplicación g de $\mathbb{R}$ en $(0, +\infty)$ definida por la misma formula, $g(x) = \exp(x)$. Consideramos estas dos aplicaciones como distintas porque tienen conjuntos de llegada diferentes. Esto nos permite decir que g es biyectiva mientras que f no lo es (ver la sección 2.2.2). ◊

Ejemplo 2.2.5.
Hay una aplicación "suma" ue asocia a cada par de enteros su suma: $(x, y) \mapsto x + y$, con conjunto de partida $\mathbb{Z} \times \mathbb{Z}$ (el conjunto de los pares de enteros) y con conjunto de llegada $\mathbb{Z}$. ◊

2.2.2 *Biyecciones*

Obsérvese que la definición de una aplicación de A en B es algo asimétrica: a cada elemento de A debe corresponder uno y sólo un elemento de B, mientras que a un elemento de B le puede corresponder uno, varios o ningún elemento de A.

Las *biyecciones* son las aplicaciones para las cuales la simetría se restablece.

Por ejemplo en la figura 2.1 de cada elemento de A sale una flecha exactamente, mientras que a cada elemento de B puede llegar una, ninguna o varias flechas.

Definicion 2.2.2. *Sea f una aplicación de A en B. Es una* biyección *cuando todo elemento de B es imagen de uno, y sólo un elemento de A.*

Ejemplo 2.2.6.

- La aplicación de $X = \{1, 2, 3\}$ en $Y = \{a, b, c, d\}$ representada por el diagrama de la figura 2.1 no es una biyección. En efecto, hay elementos sin antecedentes (como b por ejemplo). También hay un elemento con más de un antecedente (el elemento d).

- Al contrario, la aplicación de $X = \{1,2,3,4\}$ en $Y = \{A,B,C,D\}$ representada por el diagrama de la figura 2.2 es una biyección.
- Contar los elementos de un conjunto finito es establecer una biyección del conjunto de un conjunto de la forma $\{1,2,3,\ldots,n\}$.
- Las herramientas de medida físicas utilizan biyecciones entre magnitudes físicas (por ejemplo entre temperatura y altura de una columna de alcohol para un termómetro).
- Hay 4 aplicaciones del conjunto $\{1,2\}$ en él mismo. Dos de ellas son biyecciones, las otras dos no. Ver el cuadro 2.1.

$\Diamond$

Figura 2.2: esta aplicación es una biyección.

x	1	2
$f_1(x)$	1	2

x	1	2
$f_2(x)$	2	1

x	1	2
$f_3(x)$	1	1

x	1	2
$f_4(x)$	2	2

Cuadro 2.1: Las cuatro aplicaciones f_1, f_2, f_3, f_4 de $\{1,2\}$ en él mismo son las aplicaciones representadas por estas tablas. Solamente f_1 y f_2 son biyecciones.

2.2.3 *El principio de la biyección*

Regla 1. *(Principio de la biyección) Sean A y B dos conjuntos finitos. Si existe una biyección de A en B entonces A y B tienen mismo cardinal.*

Ejemplo 2.2.7. Continuación del ejemplo 2.1.1
Consideramos otra vez los dos problemas:

- Contar las maneras de repartir 12 canicas idénticas entre 5 niños.
- Contar los números de 16 bits con exactamente cuatro "1".

Mostramos, de manera más formal, que tienen el mismo número de soluciones. Sea A el conjunto de todas las maneras posibles de repartir las 12 canicas entre los 5 niños. Una repartición esta caracterizada por los números de canicas x_1, x_2, x_3, x_4, x_5 recibidas por cada niño.

Sea B el conjunto de los números de 16 bits con exactamente cuatro "1".

Definimos una aplicación $f : A \to B$ de la manera siguiente:

$f(x_1, x_2, x_3, x_4, x_5)$ es el número que se escribe:

$$\overbrace{00\cdots0}^{x_1}1\overbrace{00\cdots0}^{x_2}1\overbrace{00\cdots0}^{x_3}1\overbrace{00\cdots0}^{x_4}1\overbrace{00\cdots0}^{x_5}$$

Por ejemplo: $f(2,2,0,5,3) = 0010011000001000$.

Vemos que todo número de 16 bits con cuatro 1 es imagen de uno, y sólo un elemento $(x_1, x_2, x_3, x_4, x_5)$ de A: x_1 es el número de ceros que preceden el primer "1", x_2 es el número de ceros entre el primero y el segundo "1", ... Por lo tanto f es una biyección de A en B. Por el principio de la biyección, A y B tienen el mismo número de elementos. $\Diamond$

Hay una formula general para contar las soluciones de los problemas de distribución de este tipo, algo como $\binom{m+n-1}{m}$. Aconsejo fuertemente *no* memorizar esta formula y, en cambio, aprender este razonamiento. Una vez que hemos reducido el problema a un problema de contar cadenas de bits, sabemos que coeficiente binomial utilizar. Estos repartos de m objetos en n grupos se llaman a veces *combinaciones con repeticiones de n elementos tomados de m en m*.

Ejemplo 2.2.8.
Un objeto se desplaza en el plano, empezando en $(0,0)$. Cada paso es de longitud 1. Es o bien un paso hacia el norte (vector $(0,1)$) o bien un paso hacia el este (vector $(1,0)$). Sean m y n dos enteros positivos. ¿ Cuántas maneras posibles tiene el punto de llegar al punto (m,n) ? Por ejemplo, la parte izquierda de la figura 2.3 representa todas las soluciones para $m = 4, n = 2$.

Para contestar, asociamos a cada trayectoria la sucesión de pasos (N para norte o E para este) realizados. Observamos que cuando el objeto

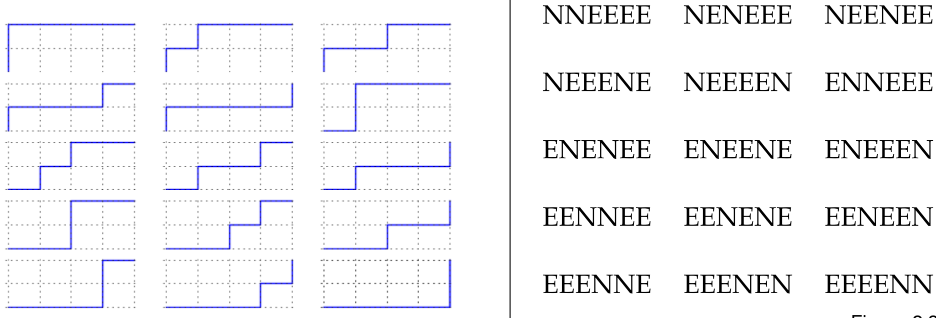


Figura 2.3: a la izquierda, los caminos que van de $(0,0)$ a $(4,2)$ con pasos unidad Norte y Este; y a la derecha las sucesiones de pasos que les corresponden.

llega al punto (m,n), es que ha hecho exactamente m pasos hacia el este y n pasos hacia el norte. Sea A el conjunto de todas las trayectorias que llegan a (m,n) y sea B el conjunto de las palabras hechas con m "E" y n "N". Sea f la aplicación de A en B que a cada trayectoria asocia su sucesión de pasos. Esta aplicación es una biyección, ya que para cada sucesión con m "E" y n "N", hay una y solamente una trayectoria llegando a (m,n) con esta sucesión. Por el principio de la biyección, A y B tienen el mismo número de elementos. Es el número de elecciones posibles de las posiciones de los n "E" entre las $m+n$ posiciones posibles. Viene dado por el coeficiente binomial $\binom{m+n}{n}$, como lo veremos más adelante.

La figura 2.3 representa esta biyección en el caso $(m,n) = (4,2)$. $\diamond$

El estudiante que llega en primer curso de grado tiene, en general, la idea que todo objeto matemático tiene que definirse por medio de *formulas* ¡ Es falso ! Muchos objetos matemáticos se describen mejor en castellano, como la aplicación f del ejemplo 2.2.8.

2.2.4 *Estrategia: contar sucesiones finitas*

La estrategia para contar presentada en este curso es la siguiente:

1. Vamos a desarrollar técnicas para contar un tipo muy especial de objetos matemáticos: las sucesiones finitas.

2. Cada vez que encontremos un problema de recuento, reduciremos el problema a un recuento de sucesiones. Más precisamente, buscaremos una biyección entre el conjunto a contar y un conjunto de sucesiones. Es lo que hemos hecho en los ejemplos 2.1.1 y 2.2.8.

Llamamos *sucesiones* a las colecciones ordenadas de objetos como las siguientes:

- $(0,0,1,0,1,1,0)$, un ejemplo de sucesión de bits. A veces lo escribimos simplemente 0010110, y lo llamamos "cadena de bits".

- $(12,15,-3,5,7)$, un ejemplo de sucesión de números.

- (C,A,S,C,A,R,A) y (R,O,M,A) son ejemplos de sucesiones de caracteres. Las escribimos a veces sin las paréntesis no las comas: CASCARA, ROMA, y en este caso las llamamos también "cadenas de caracteres" o "palabras".

El orden importa: la sucesión (R,O,M,A) es distinta de (A,M,O,R). Por esto marcamos la sucesión con paréntesis "$(\ldots)$" en vez de llaves "$\{\ldots\}$". También una sucesión no tiene por que tener términos distintos.

Los ejemplos anteriores son ejemplos de sucesiones finitas. Las sucesiones infinitas existen también, pero no las encontraremos en el estudio de este tema.

Observése que las sucesiones de longitud 2 son los *pares ordenados* mencionados en la definición 1.2.1. Extendemos esta definición a más de dos conjuntos:

Definicion 2.2.3. *Dados los conjuntos A_1, A_2, ..., A_n, entonces el conjunto de todas las sucesiones de longitud n cuyo primer término pertenece a A_1, segundo término a A_2, ..., n–ésimo término a A_n se llama* producto cartesiano *de los conjuntos A_1, A_2, ..., A_n. Se nota $A_1 \times A_2 \times \cdots \times A_n$.*

El producto cartesiano $\mathbb{R}^n$ es el ámbito natural de la geometría.

El producto cartesiano de n veces el mismo conjunto A se puede notar A^n en vez de $A \times A \times \cdots \times A$. Sus elementos son las sucesiones de longitud n cuyos términos pertenecen todos a A. Les llamamos a veces *palabras de longitud n sobre el alfabeto A*. Tienen una interpretación más: son también las aplicaciones de $\{1, 2, \ldots, n\}$ en A. Por ejemplo, si $A = \{c, a, s, r\}$, entonces "cascara" es un elemento de A^7, y la aplicación correspondente es la aplicación f de $\{1, 2, 3, 4, 5, 6, 7\}$ en $\{c, a, s, r\}$ que asocia a los cada número k la k-ésima letra de "cascara". O sea, es la aplicación que cumple $f(1) = c$, $f(2) = a$, $f(3) = s$, $f(4) = c$, $f(5) = a$, $f(6) = r$ y $f(7) = a$.

Hay un nombre más para estos objetos: *variaciones con repeticiones.*

Ejemplo 2.2.9.
Las cuatro aplicaciones de $\{1, 2\}$ en él mismo, del cuadro 2.1, se representan también como las palabras: "12", "21", "11" y "22". ♢

2.3 *El principio de adición*

Ejemplo 2.3.1.
Entre los enteros del 1 al 100, los que son múltiplos de 13 o de 17 son $7 + 5 = 12$, porque hay 7 múltiplos de 13 (ya que el cociente en la división de 100 entre 13 es 7), hay 5 múltiplos de 17 (ya que el cociente en la división de 100 entre 17 es 5), y no hay ningún múltiplo común de 13 y de 17.

En cambio, entre los números del 1 al 1000, hay 76 múltiplos de 13 y 58 múltiplos de 17, pro el número de múltiplos de 13 o de 17 no es $76 + 58$, ya que existen múltiplos comunes de 13 y de 17 que son contados dos veces en esta suma. ♢

Este ejemplo ilustra el caso más simple del *principio de adición*: si dos conjuntos A y B son disjuntos (es decir su intersección es vacía), se verifica que

$$|A \cup B| = |A| + |B|$$

Presentamos ahora la forma más general de este principio. Decimos de conjuntos A_1, A_2, ..., A_n que son *disjuntos dos a dos* (o *mutuamente disjuntos*) si cada par de estos conjuntos tiene intersección vacía: $A_1 \cap A_2 = \emptyset$, $A_1 \cap A_3 = \emptyset$, $A_2 \cap A_3 = \emptyset$, ...

Obsérvese que "mutuamente disjuntos" *no* es equivalente a que la intersección $A_1 \cap A_2 \cap A_3 \cdots$ sea vacía.

Ejemplo 2.3.2.
Los intervalos abiertos $I = (0,1)$, $J = (1,2)$ y $K = (2,3)$ son disjuntos dos a dos porque $I \cap J = \emptyset$ y $I \cap K = \emptyset$ y $J \cap K = \emptyset$ (¡ Hay que comprobar que las tres intersecciones son vacías !).

Los intervalos $M = [0,1]$, $N = [1,2]$ y $P = (2,3)$ son disjuntos (es decir $M \cap N \cap P = \emptyset$), pero no son disjuntos dos a dos: $M \cap N = \{1\}$. ♢

Regla 2. *(Principio de adición) Si los conjuntos A_1, A_2, ..., A_n son disjuntos dos a dos, entonces*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

¿ Y cuando los conjuntos no son disjuntos dos a dos, no podemos decir nada sobre el número de elementos de la unión ? ¿No hay formula ?
– Si, hay. Es más complicada pero la presentaremos en la sección 2.8.

Ejemplo 2.3.3.
Entre los enteros del 1 al 100, los que son múltiplos de 13, 15, 17 o 19 son $7 + 6 + 5 + 5 = 33$ porque:

- Hay 7 múltiplos de 13, hay 6 múltiplos de 15, hay 5 múltiplos de 17 y 5 múltiplos de 19.
- No hay múltiplo común para 13 y 15, ni para 13 y 17, ni para 13 y 19, ni para 15 y 17, ni para 15 y 19, ni para 17 y 19.

♢

2.4 El principio de multiplicación

2.4.1 El principio de multiplicación

Ejemplo 2.4.1.
¿ Cuántas palabras de longitud 4 podemos formar con las letras a, c, s ?

Solución: Tenemos 3 posibilidades para cada una de las letras. Obtenemos $3 \times 3 \times 3 \times 3 = 3^4 = 81$ palabras posibles. ♢

Ejemplo 2.4.2.
En una promoción de 50 estudiantes, se reparten un primer premio, un segundo premio y un tercer premio. ¿ Cuales son los repartos posibles ?

Solución: Hay 50 posibilidades para atribuir el primer premio. Para atribuir el segundo premio solamente hay 49 posibilidades, ya que hay que excluir el laureado del primer premio. Y para atribuir el tercer premio quedan solamente 48 posibilidades. Hay por lo tanto $50 \times 49 \times 48$ repartos posibles. ♢

Son dos ejemplos de aplicación del principio de multiplicación que enunciamos a continuación.

Regla 3 (Principio de multiplicación)**.** *Sea S un conjunto de sucesiones de longitud n tal que haya:*

- *k_1 elecciones posibles para el primer término.*

- *Para cada elección de primer término, k_2 elecciones posibles para el segundo término.*
- *Para cada elección de los dos primeros términos, k_3 elecciones posibles para el tercer término.*
- *...*

Entonces S tiene $k_1 \cdot k_2 \cdot k_2 \cdots k_n$ elementos.

2.4.2 *El cardinal del producto cartesiano, y el número de subconjuntos de un conjunto*

Este principio tiene dos aplicaciones particularmente interesantes, que detallamos a continuación.

Cuando las elecciones para el primer término forman un conjunto A_1, las elecciones para el segundo término forman un conjunto A_2, ... y las elecciones de los diferentes términos son independientes entre si. Entonces S es exactamente el producto cartesiano $A_1 \times A_2 \times \cdots \times A_n$. Es el caso del ejemplo 2.4.1, con $A_1 = A_2 = A_3 = A_4 = \{a, c, s\}$. Obtenemos que el cardenal del producto cartesiano es el producto de los cardenales:

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$$

Un caso particular es cuando todos los conjuntos A_i son iguales a un mismo conjunto A. Entonces obtenemos:

$$|A^n| = |A|^n$$

Recordar que este conjunto A^n tiene las interpretaciones siguientes:

- El conjunto de las palabras de longitud n en el alfabeto A (es decir, el conjunto de las sucesiones de longitud n con términos en A).
- El conjunto de todas las aplicaciones de $\{1, 2, \ldots, n\}$ en A.

Los estudiantes en informática deberían conocer las primeras potencias de 2:

1
2
4
8
16
32
64
128
256
512
1024
2048
4096
8192
16384
32768
65536

En particular, es útil saber que $2^{10} \approx 1000$.

Ejemplo 2.4.3.
Pregunta: ¿ Cuántos subconjuntos tiene $\{1, 2, 3, \ldots, 10\}$?

Solución: sea S el conjunto de los subconjuntos de $\{1, 2, 3, \ldots, 10\}$ y B el conjunto de las sucesiones de 10 bits. Definimos una biyección de S en B de la manera siguiente: a un subconjunto T de $\{1, 2, 3, \ldots, 10\}$ asociamos la sucesión $a_1 a_2 \cdots a_{10}$ donde $a_i = 1$ si $i \in T$, sino $a_i = 0$. Por ejemplo a $T = \{1, 5, 7, 10\}$ se asocia: 1000101001.

Por el principio de la biyección, tenemos $|S| = |B|$. Ahora B es simplemente $\{0, 1\}^{10}$. Por lo tanto $B = 2^{10} = 1024$. En conclusión, el conjunto $\{1, 2, 3, \ldots, 10\}$ tiene 1024 subconjuntos. ◊

Razonando de manera similar para un conjunto con un número n cualquiera de elementos, obtenemos el resultado siguiente:

Teorema 2.4.1. *Un conjunto de n elementos tiene exactamente 2^n subconjuntos.*

Ejemplo 2.4.4.
¿ Cuántas aplicaciones hay de $\{1,2,3\}$ en $\{1,2,3,4,5,6\}$?

Solución: Estas aplicaciones son simplemente las palabras de longitud 3 en el alfabeto $\{1,2,3,4,5,6\}$. Por lo tanto hay 6^3 tales aplicaciones. $\lozenge$

Ejemplo 2.4.5.
De manera general, vemos que el número de aplicaciones del conjunto finito X al conjunto finito Y es $|Y|^{|X|}$. $\lozenge$

2.4.3 *El principio de adición y el principio de multiplicación juntos*

Ejemplo 2.4.6.
En este ejemplo se aplica tanto el principio de adición como el principio de multiplicación.

En cierto sistema informático, una contraseña válida tiene entre 6 y 8 caracteres válidos. El primero tiene que ser un carácter alfabético, los siguientes son alfabéticos o numéricos. Hay 52 caracteres alfabéticos autorizados. Son:

$$A = \{a, b, c, \ldots, z, A, B, C, \ldots, Z\}$$

y 10 caracteres numéricos autorizados:

$$N = \{0, 1, 2, \ldots, 9\}$$

Pregunta: ¿ Cuántas contraseñas válidas hay ?

Solución: Sea k el número de contraseñas válidas, es el número que buscamos. Sea $S = A \cup N$. El conjunto de las contraseñas validas es:

$$(A \times S^5) \cup (A \times S^6) \cup (A \times S^7)$$

Las contraseñas en $A \times S^5$ son las de 6 caracteres (como por ejemplo "Z34pp1"; "Z" está en A y "34pp1" está en S^5), las contraseñas en $A \times S^6$ tienen longitud 7 y las contraseñas en $A \times S^7$ tienen longitud 8. Como estos tres conjuntos son disjuntos dos a dos, podemos aplicar el principio de adición;

$$k = |A \times S^5| + |A \times S^6| + |A \times S^7|$$

Luego aplicando la regla de multiplicación obtenemos:

$$k = |A| \cdot |S^5| + |A| \cdot |S^6| + |A| \cdot |S^7|$$

Aplicando el principio de adición para $S = A \cup N$ (ya que A y N son disjuntos), obtenemos $|S| = |A| + |N| = 52 + 10 = 62$. Finalmente:

$$k = 52 \cdot 62^5 + 52 \cdot 62^6 + 52 \cdot 62^7 \cong 1,8 \cdot 10^{14} \text{ contraseñas posibles.}$$

$\lozenge$

2.4.4 *Palabras sin repetición y permutaciones*

Aplicamos ahora la regla de multiplicación para contar las palabras sin repetición, como *abc*, *abd*, *cba*, ... pero no *aba* (repetición de *a*).

¿ Cuántas son las palabras sin repetición de longitud n sobre un alfabeto de k elementos ? Tenemos:

- k elecciones posibles para la primera letra,
- Para cada elección posible de primera letra, $k-1$ elecciones posibles para la segunda letra.
- Para cada elección de las dos primeras letras, $k-2$ elecciones posibles de tercera letra.
- ...

Por lo tanto:

Teorema 2.4.2. *El número de palabras de longitud n, sin repetición de letras, sobre un alfabeto de k elementos es:*

$$k(k-1)(k-2)\cdots(k-n+1)$$

Obsérvese que es un producto de n términos.

Las palabras sin repetición se llaman a veces *variaciones sin repetición*.

"Sobre un alfabeto de k elementos" significa que tenemos a nuestra disposición este número de letras. Por ejemplo, las cadenas de bits son las palabras sobre el alfabeto $\{0,1\}$.

Ejemplo 2.4.7.
¿Cuántos números de 3 cifras existen sin cifras repetidas ? Respuesta: $10 \times 9 \times 8 = 720$, puesto que hay 10 posibles elecciones para el primer dígito, 9 para el segundo y 8 para el tercero. ◊

Una caso particular del recuento anterior es él de las palabras de longitud n sin repetición sobre un alfabeto de n elementos (mismo n). Estas palabras se llaman *permutaciones* del alfabeto.

Ejemplo 2.4.8.
¿Cuántos números de tres cifras distintas se pueden escribir con los dígitos 1, 3, 5? Respuesta: son las 6 permutaciones de $\{1,3,5\}$, a saber:

$$\begin{array}{ccc} 135, & 153, & 315, \\ 351, & 513, & 531 \end{array}$$

◊

Como caso particular de la formula para contar las palabras sin repetición de longitud n sobre un alfabeto dado, vemos que el número de permutaciones de un conjunto de n elementos es:

$$n(n-1)(n-2)\cdots 2\cdot 1$$

Es el producto de los n primeros enteros no–negativos (el *factorial de* n, notada $n!$). Lo enunciamos como teorema.

Teorema 2.4.3. *El número de permutaciones de un conjunto de n elementos es $n!$.*

Importante: el factorial de 0 se define como: $0! = 1$. Es consistente con el Teorema.

Los primeros factoriales:

1
1
2
6
24
120
720
5040
40320
362880
3628800
39916800
479001600
6227020800
87178291200
1307674368000
20922789888000
355687428096000
6402373705728000
121645100408832000
2432902008176640000

Ejemplo 2.4.9.
¿ Cuántas son las permutaciones (=anagramas) de la palabra CONTAR ? Ya que CONTAR no tiene letra repetida, son las 6! permutaciones del conjunto $\{C, O, N, T, A, R\}$. Se llaman también *permutaciones del conjunto* $\{C, O, N, T, A, R\}$. ♢

Hemos visto que las palabras de longitud n sobre A se identifican con las aplicaciones de $\{1, 2, \ldots, n\}$ en A. Bajo esta identificación, las permutaciones de A se corresponden con las *biyecciones* de $\{1, 2, \ldots, n\}$ en A.

2.5 El principio de división

2.5.1 El principio de división

Ejemplo 2.5.1.
Queremos montar una red local de 8 ordenadores en anillo doble, es decir como en la figura 2.4. Los ordenadores, con números de 1 hasta 8, tienen características diferentes. ¿ Cuántas redes diferentes se pueden montar ? Consideramos dos redes como idénticas si tienen la misma topología (es decir: si cada ordenador tiene los mismos vecinos en las dos redes). La topología de una red es importante porque determina que ordenadores se comunican más rápidamente entre sí, y el comportamiento de la red en caso de ruptura de cables.

Intentando reducir el problema a un problema de conteo de sucesiones, podemos introducir la aplicación f que a una permutación de $\{1, 2, \ldots, 8\}$ asocia la configuración donde el ordenador etiquetado con el primer número de la permutación esta en la posición más alta del anillo, el ordenador etiquetado con el segundo número inmediatamente a su derecha . . . (por ejemplo la configuración de la figura 2.4viene de la permutación 13276845) pero, por cierto, no es una biyección (la configuración de la figura 2.4 es la misma que la configuración obtenida de la permutación 23768451 por ejemplo) . . . ♢

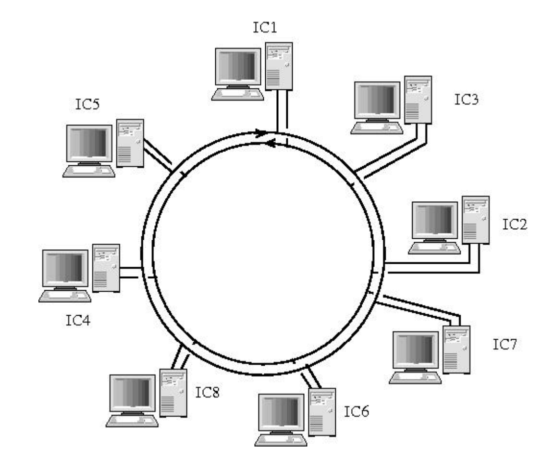


Figura 2.4: Ejemplo 2.5.1.

Vamos a introducir una regla más, para refinar el principio de biyección y resolver problemas como el anterior.

Definicion 2.5.1. *Una aplicación $f : A \to B$ es* de grado combinatorio k *si todo elemento del conjunto de llegada B tiene exactamente k antecedentes.*

Obsérvese que las aplicaciones de grado combinatorio 1 son exactamente las aplicaciones biyectivas.

Regla 4 (Principio de división). *Si $f : A \to B$ es de grado combinatorio k entonces $|A| = k \cdot |B|$.*

Ejemplo 2.5.2.
Seguimos con el ejemplo 2.5.1.

Contamos las permutaciones de $\{1, 2, \ldots, 8\}$ que dan lugar a la misma topología de la red. Son todas las sucesiones de ordenadores que encontramos recorriendo el anillo de una manera u otra. Para una topología de red dada podemos:

- Elegir arbitrariamente un "primer" ordenador en el anillo (8 posibilidades).
- Para cada primer ordenador, podemos elegir uno o el otro sentido para recorrer el anillo (2 posibilidades).

Por el principio de multiplicación, hay 16 permutaciones que corresponden a una topología de red dada.

Aplicando ahora el principio de división, con el conjunto de las permutaciones de $\{1, 2, \ldots, 8\}$ para A, el conjunto de las topologías de red para B, y la aplicación f definida en el ejemplo 2.5.1, vemos que $|B| = |A|/16 = 8!/16 = 2520$. ♢

2.5.2 *El recuento de los subconjuntos de k elementos de un conjunto de n elementos*

Ejemplo 2.5.3.
¿ Cuántas manos de poker se pueden obtener de un juego de 52 cartas ?

Un mano de poker es cualquier conjunto de 5 cartas. Para contarlas, consideramos en primer lugar las *sucesiones* de 5 cartas, que sabemos contar: son $52 \times 51 \times 50 \times 49 \times 48$ por el principio de multiplicación. Sea S el conjunto de todas las sucesiones (con orden) de 5 cartas extraídas del juego de 52 cartas, y C el conjunto de todos los conjuntos (sin orden) de 5 cartas extraídos del juego. Sea f la aplicación de S en C que olvida el orden. Por ejemplo,

$$f((5\clubsuit, 1\heartsuit, K\diamondsuit, Q\diamondsuit, 10\diamondsuit)) = f((1\heartsuit, 5\clubsuit, K\diamondsuit, Q\diamondsuit, 10\diamondsuit)) = \ldots = \{5\clubsuit, 1\heartsuit, K\diamondsuit, Q\diamondsuit, 10\diamondsuit\}$$

Dado un conjunto de 5 cartas, ¿ Cuántos antecedentes tiene por f ? Respuesta: son todas las permutaciones del conjunto, son $5!$. Por lo tanto f es de grado combinatorio $5!$. Por el principio de división, el cardinal de C es:

$$|C| = \frac{|S|}{5!} = \frac{52 \times 51 \times 50 \times 49 \times 48}{5!} \cong 2,6 \text{ milliones}$$

♢

Lo que hemos hecho en este ejemplo es contar todos los subconjuntos de 5 elementos de un conjunto de 52 elementos.

Los subconjuntos de k elementos de un conjunto dado A se llaman a veces *combinaciones de elementos de A tomados de k en k*. Los números de combinaciones de n elementos tomados de k en k son omnipresentes en matemática, al punto de tener un nombre: *coeficientes binomiales*, y un símbolo especial: $\binom{n}{k}$.

En $\binom{n}{k}$ ponemos el grande número n arriba, el pequeño k abajo.

Aplicando el principio de división como en el ejemplo 2.5.3, obtenemos las formulas siguiente para los coeficientes binomiales.

Teorema 2.5.2. *Los coeficientes binomiales $\binom{n}{k}$ verifican la formula:*

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+2)(n-k+1)}{k!}$$

Obsérvese que el numerador se puede escribir:

$$n(n-1)(n-2)\cdots(n-k+2)(n-k+1) = \frac{n!}{(n-k)!}$$

Por lo tanto, el coeficiente binomial cumple también:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{2.1}$$

Ejemplo 2.5.4.
Calculemos $\binom{10}{5}$. Tenemos:

$$\binom{10}{5} = \frac{10 \times 9 \times 8 \times 7 \times 6}{5 \times 4 \times 3 \times 2 \times 1}$$

Podemos simplificar eliminando factores comunes del numerador y del denominador:

¡Ni necesitamos calculadora !

$$\begin{aligned}\binom{10}{5} &= \frac{10 \times 9 \times 8 \times 7 \times 6}{5 \times 4 \times 3 \times 2 \times 1} \\ &= \frac{(2 \times 5) \times (3 \times 3) \times (2 \times 4) \times 7 \times 6}{5 \times 4 \times 3 \times 2 \times 1} \\ &= \frac{(\not{2} \times \not{5}) \times (\not{3} \times 3) \times (2 \times \not{4}) \times 7 \times 6}{\not{5} \times \not{4} \times \not{3} \times \not{2} \times 1} \\ &= 3 \times 2 \times 7 \times 6 \\ &= 252\end{aligned}$$

◊

Desarrollaremos el estudio de los coeficientes binomiales más en detalle en la sección 2.6.

2.5.3 *Permutaciones de palabras con letras repetidas (anagramas)*

Consideramos otra aplicación del principio de división.

Ejemplo 2.5.5. (El truco de poner números a las letras)

¿ Cuántos anagramas tiene la palabras “SOSOS” ? ¿ Y “CASCARA” ?

Las mismas preguntas se formulan también así:

¿ Cuántas palabras sobre el alfabeto $\{S, O\}$ tienen 2 ocurrencias de O y tres de S ?
¿ Cuántas palabras sobre el alfabeto $\{C, A, S, R\}$ tienen 2 ocurrencias de C, 3 ocurrencias de A, 1 ocurrencia de S y una ocurrencia de R ?

Ya sabemos contar los anagramas de SOSOS (¿Por que ?) ¿ Como contar los anagramas de CASCARA ? Aplicamos el principio de división. Sea B el conjunto de los anagramas de CASCARA, es el conjunto cuyo cardinal queremos determinar. Introducimos ahora un nuevo alfabeto X, que consiste de copias distintas de sus letras: $X = \{C_1, A_1, S, C_2, A_2, R, A_3\}$. Sea B el conjunto de todas las permutaciones de X. Sea $f : A \to B$ la aplicación que "olvida los índices". Por ejemplo:

$$f(A_1C_1RSA_3C_2A_2) = ACRSACA$$

Entonces f tiene grado combinatorio:

$$3! \times 2! \times 1! \times 1!$$

En efecto, dos permutaciones de X tienen la misma imagen si y sólo si se obtienen cada una de la otra permutando las letras A_1, A_2, A_3 entre ellas y las letras C_1 y C_2 entre ellas (y necesariamente guardando la R y la S fijas)

Por el principio de división:

$$|B| = \frac{|A|}{3!2!1!1!}$$

Pero $|A| = 7!$ (permutaciones de un conjunto de 7 elementos). Por lo tanto:

$$|B| = \frac{7!}{3!2!1!1!} = 420.$$

◊

El razonamiento se generaliza, proporcionando el resultado siguiente:

Teorema 2.5.3. *El número de palabras formadas con exactamente k_1 ocurrencias de un elemento, k_2 ocurrencias de otro elemento, ..., k_r ocurrencias de un elemento distinto de todos los anteriores es:*

$$\frac{n!}{k_1!k_2!\cdots k_r!}$$

donde $n = k_1 + k_2 + \cdots + k_r$ (obsérvese que es la longitud de la palabra).

2.6 Coeficientes binomiales

El coeficiente binomial $\binom{n}{r}$ cuenta los subconjuntos de k elementos de un conjunto de n elementos. Damos a continuación unas propiedades útiles e interesantes de estos números.

Los conjuntos de k elementos de un conjunto de n elementos se llaman a veces *combinaciones (sin repetición) de n elementos tomados de k en k.*

2.6.1 Una simétria de los coeficientes binomiales

Proposición 2.6.1. *Dados dos enteros no–negativos n y k se tiene:*

$$\binom{n}{k} = \binom{n}{n-k} \tag{2.2}$$

Damos dos demostraciones de este resultado.

Demostración. Hemos establecido en (2.1)que:

$$\binom{n}{k} = \frac{n!}{k!(n-k!)}$$

Sustituyendo k por $n-k$ (y, en consecuencia, $n-k$ por $n-(n-k)$, que vale k) en esta formula obtenemos:

$$\binom{n}{n-k} = \frac{n!}{(n-k)!k!}$$

Esto es igual a $\binom{n}{k}$. □

La segunda demostración es una *demostración biyectiva* de la identidad (2.2): consiste en hallar para cada uno de los dos miembros de (2.2) un conjunto que tiene este número de elementos, y luego establecer que estos dos conjuntos están en biyección.

Demostración. Sean X (respectivamente Y) el conjunto de los subconjuntos de cardinal k (resp. $n-k$) de $\{1,2,3,\ldots,n\}$. Entonces $|X| = \binom{n}{k}$ e $|Y| = \binom{n}{n-k}$. Para todo subconjunto A de $\{1,2,3,\ldots,n\}$ a k elementos, notamos $f(A)$ para $\overline{A}$ (el complementario de A). Entonces f es una biyección de X en Y. Por lo tanto, $|X| = |Y|$. Esto establece la identidad (2.2). □

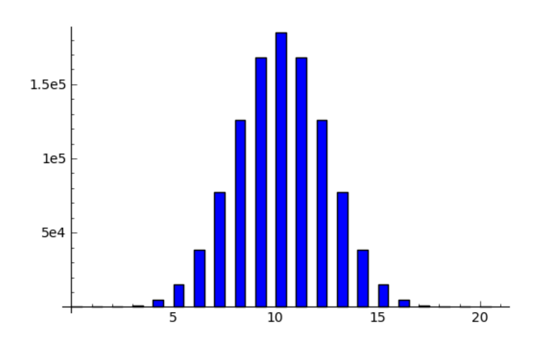


Figura 2.5: los coeficientes binomiales $\binom{20}{k}$. Obsérvese que la sucesión crece y luego decrece. Se dice que esta sucesión es *unimodal*, y es una propiedad frecuente e interesante de las sucesiones producidas por recuentos. También se aprecia la simétria de la sucesión, ver (2.2).

2.6.2 *El triángulo de Pascal*

Proposición 2.6.2. *Para todos enteros n y k con $n \geq 0$ y $k \geq 1$ se tiene:*

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \tag{2.3}$$

Demostración. Definimos los conjuntos siguientes:

- X el conjunto de todos los subconjuntos de $\{1,2,\ldots,n+1\}$.
- A el conjunto de todos los subconjuntos de $\{1,2,\ldots,n+1\}$ que contienen $n+1$.
- B el conjunto de todos los subconjuntos de $\{1,2,\ldots,n+1\}$ que no contienen $n+1$. Ó simplemente, B es el conjunto de todos los subconjuntos de $\{1,2,\ldots,n\}$.

Observamos que $X = A \cup B$, y que esta unión es disjunta. Por lo tanto (por el principio de adición), $|X| = |A| + |B|$. Tenemos $|X| = \binom{n+1}{k}$ y $|B| = \binom{n}{k}$. Para determinar $|A|$, consideramos el conjunto C de todos los subconjuntos de $\{1,2,3,\ldots,n\}$ con $k-1$ elementos. La aplicación $f : C \to A$ definida por $f(S) = S \cup \{n+1\}$ es una biyección. Por lo tanto $|C| = |A|$. Pero $|C| = \binom{n}{k-1}$. Obtenemos así la formula anunciada. □

Calculemos los primeros coeficientes binomiales y los colocamos en la tabla 2.2, llamada *triángulo de Pascal*.

Observación: Para $n = 0$ o $n = k$ se tiene siempre $\binom{n}{k} = 1$. Para $k = 1$ se tiene $\binom{n}{k} = n$.

Los coeficientes binomiales involucrados en la formula (2.3) están en la configuración siguiente:

$$\begin{array}{cc} \binom{n}{k-1} & \binom{n}{k} \\ \cdots & \binom{n+1}{k} \end{array}$$

La formula (2.3) se interpreta de la manera siguiente con respecto a esta tabla:

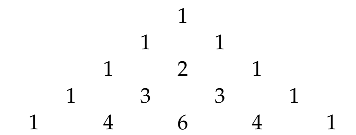
Cuadro 2.2: el triángulo de Pascal

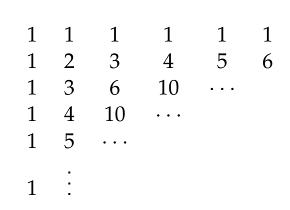
	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$n=0$	1					
$n=1$	1	1				
$n=2$	1	2	1			
$n=3$	1	3	3	1		
$n=4$	1	4	6	4	1	
$n=5$	1	5	10	10	5	1

En la tabla anterior, cada coeficiente binomial es la suma del coeficiente que esta en su norte y del que esta en su noroeste.

Nos permite por lo tanto calcular los coeficientes binomiales sucesivamente.

Obsérvese sin embargo que esta tabla esta a menudo representada con otras orientaciones, ver cuadro 2.3





Cuadro 2.3: El triángulo de Pascal, con varias orientaciones.

2.6.3 *La formula del binomio de Newton*

Las filas de las tablas anteriores suenan familiares ...

$$(x+y)^2 = x^2 + 2\,xy + y^2$$
$$(x+y)^3 = x^3 + 3\,x^2y + 3\,xy^2 + y^3$$
$$(x+y)^4 = x^4 + 4\,x^3y + 6\,x^2y^2 + 4\,xy^3 + y^4$$
$$\vdots$$

Proposición 2.6.3 (Teorema del binomio de Newton). *El coeficiente binomial $\binom{n}{k}$ es el coeficiente de $x^k y^{n-k}$ en el desarrollo de $(x+y)^n$.*

Demostración. Desarrollamos $(x+y)^n$ pero *prohibiendo cambiar el orden de los x y de los y*, es decir sin derecho a la regla de conmutación. Por ejemplo, para $n=2$ obtenemos:

$$(x+y)^2 = (x+y)\cdot(x+y) = x\cdot(x+y) + y\cdot(x+y) = xx + xy + yx + yy.$$

Como no tenemos derecho a la regla de conmutación, guardamos xy e yx separados. Igualmente para $n=3$ obtenemos:

$$(x+y)^3 = xxx + xxy + xyx + yxx + xyy + yxy + yyx + yyy$$

Obtenemos todas las palabras de longitud 3 en la letras x e y. De manera general, desarrollando el producto obtenemos una suma de términos. Cada término corresponde a una elección entre x e y para cada uno de los n factores $(x+y)$: en k-ésima posición del término obtenemos la letra x o y elegida en el k-ésimo factor $(x+y)$. Por lo tanto, lo que obtenemos son exactamente todas las palabras de longitud n en las letras x e y. Simplificamos ahora la suma, por medio de la regla de conmutación. Esta simplificación consiste en asociar a cada palabra el monomio $x^k y^{n-k}$ con el mismo número de x y de y.

DE ARTE CONJECTANDI. 3

ſolo ordine ſitúve mutato, dicentur quæri omnes permutationes rerum illarum.

Res autem permutandæ vel omnes poſſunt eſſe diverſæ, vel aliquot earum eædem; quæ quidem per totidem Alphabeti literas, ſive diverſas ſive eaſdem, commodè deſignabuntur.

1. *Si res omnes permutandæ ſunt diverſæ:*

CUM numerus permutationum in rebus pluribus iniri nequeat, niſi idem priùs in omnibus aliis numero paucioribus compertus habeatur, liquet in hâc inquiſitione utendum viâ ſyntheticâ, hoc eſt, ordiendum nobis eſſe ab hypotheſibus omnium primis & ſimpliciſſimis:

Unius rei, vel literæ, *a*, una tantùm ſumptio vel poſitio eſt.

Duarum rerum, aut literarum, *a* & *b*, vel *a* præcedit & *b* ſequitur, vel præcedente *b* ſequitur *a*; unde duo ipſarum fiunt ordines *a b* & *b a*.

Tres, porrò, literæ *a*, *b*, *c*, ita collocari poſſunt, ut primus locus vel ipſi *a* vel *b* vel *c* concedatur: ſi *a* primum tenet locum, reliquæ duæ duobus, ut diximus, modis diſponi queunt: ſi *b* in primum locum transferatur, reliquarum duarum duplex itidem poterit eſſe poſitio; quod & intelligendum, ubi tertia *c* primam ſedem occupaverit. Unde trium literarum in univerſum ter duæ, ſeu 6, exiſtunt permutationes *a b c*, *a c b*: *b a c*, *b c a*: *c a b*, *c b a*.

Similitèr, ſi 4 extent literæ *a*, *b*, *c*, *d*, earum unaquæque primum obtinere locum poteſt, intereà dum tres reliquæ, ut nunc oſtenſum, ter bis, ſeu ſexiès, ordinem variabunt: quare cùm earum, quæ primo loco poni poſſunt, ſint quatuor, ſequitur omnes quatuor quater ter bis, ſeu quater ſexies, hoc eſt, vicies quater ſitum inter ſe permutare poſſe.

Ob eandem rationem accedente 5tâ literâ *e* inſtitui poſſunt quinquies tot variationes, quot in caſu præcedenti, hoc eſt, quinquies 24, ſeu 120. Et generalitèr, datis quotcunque literis, numerus permutationum, quas ſubire poſſunt omnes, totiès excedit numerum permutationum, quas recipiunt literæ unâ pauciores, quot ſunt unitates in dato literarum numero. Unde ſponte manat ſequens

B 2 *Regula*

Para cada k, el monomio $x^k y^{n-k}$ tiene exactamente $\binom{n}{k}$ antecedentes (todas las palabras con exactamente k "x"). Por lo tanto este monomio aparece en la suma simplificada con el coeficiente $\binom{n}{k}$. □

Una forma quizás más simple del teorema del binomio de Newton es la siguiente:

El coeficiente binomial $\binom{n}{k}$ es el coeficiente de x^k en el desarrollo de $(1+x)^n$.

Se obtiene de la versión anterior sustituyendo y por 1.

Se puede utilizar esta propiedad como *definición* de los coeficientes binomiales. En este caso, tiene sentido considerar $\binom{n}{k}$ con k negativo (vale 0).

2.7 El principio del palomar

2.7.1 Principio de comparación. Aplicaciones inyectivas y aplicaciones sobreyectivas

La condición que define "función biyectiva" (todo elemento de B es imagen de uno, y sólo un, elemento de A) puede partirse en dos ("uno por lo menos" de un lado, "no más de un" por el otro lado), dando lugar a dos tipos de aplicaciones las aplicaciones *inyectivas* y las aplicaciones *sobreyectivas*.

Definicion 2.7.1. *Sea f una función de A en B.*

- *Decimos que f es* inyectiva *cuando cada elemento del conjunto de llegada B es imagen de,* a lo más, *un elemento del conjunto de partida A.*
- *Decimos que f es* sobreyectiva *cuando cada elemento del conjunto de llegada B es imagen de* al menos *un elemento del conjunto de partida A.*

Obsérvese que una aplicación es biyectiva si y sólo si es inyectiva y sobreyectiva a la vez.

Para entender las nociones de "aplicación inyectiva" y "aplicación sobreyectiva", puede ser útil enunciar lo que es para una aplicación $f : A \to B$ *no* ser inyectiva o *no* ser sobreyectiva:

- La aplicación f no es inyectiva si y sólo si existen dos elementos del conjunto de partida A que tienen la misma imagen: $f(a) = f(a')$ con $a \neq a'$.
- La aplicación f no es sobreyectiva si y sólo si existe un elemento del conjunto de llegada B que no sea la imagen de ningún elemento del conjunto de partida A.

Ejemplo 2.7.1.
Hemos visto (parágrafo 2.2.4) que las aplicaciones con conjunto de partida $\{1, 2, \ldots, n\}$ se identifican con las palabras de longitud n. Vemos que en esta identificación, las aplicaciones *inyectivas* corresponden a las palabras *sin repetición*. ♢

Ejemplo 2.7.2.
Los diagramas de la figura 2.6 proporcionan ejemplos respectivamente de:

- aplicación ni inyectiva (d tiene dos antecedentes), ni sobreyectiva (b no tiene antecedente).
- aplicación inyectiva pero no sobreyectiva (C no tiene antecedente).
- aplicación sobreyectiva pero no inyectiva (C tiene dos antecedentes):
- aplicación a la vez inyectiva y sobreyectiva, es decir: biyectiva.

◊

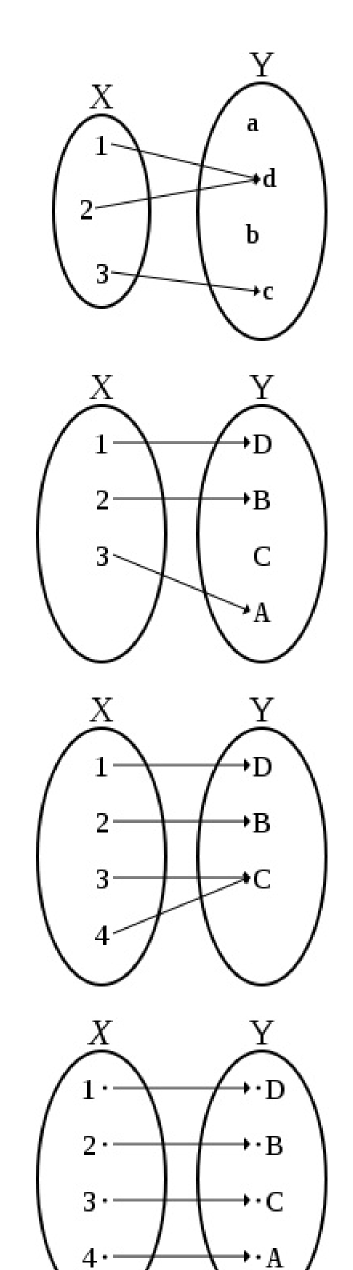


Figura 2.6: ejemplos de aplicaciones: arriba: ni inyectiva, ni sobreyectiva; luego: inyectiva pero no sobreyectiva; luego: sobreyectiva pero no inyectiva; y abajo: biyectiva.

Regla 5 (Principio de comparación). *Sea f una aplicación de A en B.*

- *Si f es inyectiva entonces $|A| \leq |B|$.*
- *Si f es sobreyectiva entonces $|A| \geq |B|$.*

2.7.2 *El principio del palomar*

Ejemplo 2.7.3.
Si 100 palomas vuelan hacia los 99 nichos de un palomar, entonces por lo menos en uno de los nichos habrá dos o más palomas. ◊

No hace falta seguir la clase de IMD para saber esto ... pero si la misma idea se aplica al problema siguiente, ¿ Suena más interesante ?

Ejemplo 2.7.4.
Considérese los 60 números de 15 cifras siguientes:

887964719632934	853595052833373	353509619982551	830081730551540
558079829715801	307576632323256	959631796100512	280379210953414
287229227755456	614322636818484	477470770159150	964060126349588
185696359139546	574393100402120	358758104182863	843847375041982
704043291794585	164943283221929	932251176700079	842476365687260
129996517563239	241354310206714	107264753201775	430048151603065
918930703766236	933789763806865	262826621816025	764046725256856
203255531597317	965760785214437	247116472139512	155568031850258
196140160830560	598577947802257	800411246266011	246457748356885
117050842616421	737669914029536	740543467620656	271869513523706
471598056079794	701491105472926	921393733200788	668448572075951
895397921831942	748605058193416	372197002112284	926502765039260
793443436342175	627143070588176	191487778595898	172981291280290
812999090787980	815653706272151	807868444440746	959818069149332
809176361839847	279183905034511	580827257466009	237622287732636

Afirmamos que existen dos subconjuntos de este conjunto de números, disjuntos y con la misma suma ... ◊

La idea del ejemplo 2.7.3 se formaliza de la manera siguiente:

Regla 6 (Principio del palomar)**.** *Si* $|A| > |B|$ *entonces ninguna función* $f : A \to B$ *es inyectiva. Es decir, para toda aplicación* $f : A \to B$*, existen dos elementos distintos del conjunto de partida* A *con la misma imagen por* f*.*

Obsérvese que esta regla no es otra cosa que el contrarrecíproco del principio de comparación para funciones inyectivas (parágrafo anterior).

Ejemplo 2.7.5.
Demostramos ahora la afirmación hecha en el ejemplo 2.7.4. Las palomas serán los conjuntos de números de la lista, los nichos serán sus sumas.

Cada número de la lista es inferior a 10^{15}, y hay 60 números en la lista. Por lo tanto, la suma de todos les elementos de la lista es inferior a 60×10^{15}. Este número es también, claro, una cota superior para la suma de los elementos de cualquier subconjunto del conjunto de los números de la lista. Consideremos la aplicación f que a cada uno de estos subconjuntos asocia la suma de sus elementos. Toma sus valores en $\{1, 2, \ldots, 60 \times 10^{15}\}$. Tenemos $2^{60} > 60 \times 10^{15}$ (en efecto, $2^{10} = 1024 > 1000$, por lo tanto $2^{60} = (2^{10})^6 > (10^3)^6 = 10^{18}$, y, por otra parte, $10^{18} > 60 \times 10^{15}$). Por el principio del palomar, existen dos subconjuntos A y B del conjunto de los 60 números con la misma suma. Los conjuntos A y B no son necesariamente disjuntos. Pero los conjuntos $A \setminus B$ y $B \setminus A$ lo son, y también tienen la misma suma. ♢

2.7.3 *El principio del palomar, generalizado*

El principio del palomar admite (entre otras) la siguiente generalización:

Regla 7 (Principio del palomar generalizado)**.** *Si* $|A| > k|B|$ *entonces para toda aplicación* $f : A \to B$*, existen* $k+1$ *elementos de* A *que tienen la misma imagen por* f*.*

Ejemplo 2.7.6.
En Sevilla capital hay poco más de 700 000 personas, y ciertamente más de 600 000 personas que no son calvas. Entre ellas, hay por lo menos cuatro personas que tienen *exactamente* el mismo número de cabellos. En efecto, nadie tiene más de 200 000 pelos. Sea A el conjunto de los sevillanos no calvos y $B = \{1, 2, \ldots, 200\,000\}$. Tenemos $|A| > 600\,000 \geq 3 \cdot |B|$. Sea $f : A \to B$ la aplicación que a cada sevillano no calvo asocia su número de pelos. Se aplica el principio del palomar generalizado. ♢

2.8 *El principio de inclusión y exclusión*

En el parágrafo 2.3 hemos contado los elementos de la unión de conjuntos, cuando son disjuntos dos a dos. Aquí examinamos el caso general, quitando la restricción "disjuntos dos a dos".

Ejemplo 2.8.1. Continuación del ejemplo 2.3.1
Queremos contar lo enteros del 1 al 1000 que son múltiplos de 13 o de 17. Hay 76 múltiplos de 13 y 58 múltiplos de 17 en este intervalo. Pero en la suma $76 + 58$ no contamos bien los múltiplos de 13 o de 17, ya que contamos *dos veces* sus múltiplos comunes. Tenemos que restar una vez los múltiplos comunes de 13 y de 17 para obtener la cuenta correcta:

$76 + 58 -$ número de multiplos comunes de 13 y de 17 entre 1 y 1000.

Veremos en la parte "aritmética" (Tema 4) que los múltiplos comunes de 13 y 17 son exactamente los múltiplos de 13×17, que vale 221. Hay 4 múltiplos de 221 entre 1 y 1000. Por lo tanto el número de múltiplos de 13 o 17 entre 1 y 1000 es $76 + 58 - 4 = 130$. $\diamondsuit$

Enunciamos el resultado general:

Sean A y B dos conjuntos. Entonces:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Demostración. Basta con descomponer $A \cup B$ como unión de subconjuntos disjuntos dos a dos y luego aplicar el principio de la suma. Tenemos:

$$A \cup B = (A \setminus (A \cap B)) \cup (B \setminus (A \cap B)) \cup (A \cap B)$$

y los conjuntos a la derecha son disjuntos dos a dos. Por lo tanto:

$$|A \cup B| = |A \setminus (A \cap B)| + |B \setminus (A \cap B)| + |A \cap B|$$

Tenemos también: $A = (A \cap B) \cup (A \setminus (A \cap B))$ con los conjuntos de la derecha disjuntos. Otra vez por el principio de adición: $|A| = |A \cap B| + |A \setminus (A \cap B)|$. Por lo tanto: $|A \setminus (A \cap B)| = |A| - |A \cap B|$. Similarmente, $|B \setminus (A \cap B)| = |B| - |A \cap B|$. Obtenemos así:

$$|A \cup B| = |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B| = |A| + |B| - |A \cap B|$$

$\square$

En el caso de tres conjuntos hay una formula similar.

Sean A, B y C tres conjuntos. Entonces:

$$\begin{aligned} |A \cup B \cup C| = {} & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C| \end{aligned}$$

Ejemplo 2.8.2. (El truco de reunir letras.)
¿ Cuántas permutaciones del conjunto $\{0, 1, 2, \ldots, 9\}$ contienen, consecutivamente y en este orden: "4" y luego "2", o "0" y luego "4", o "6" y luego "0" ?

Por ejemplo, 9516243870 no conviene, pero 9516042387 si.

Solución: Sea P_{42} el conjunto de las permutaciones que contienen "42". Sea P_{04} el conjunto de las permutaciones que contienen "04", y P_{60} el conjunto de las permutaciones que contienen "60". Estamos buscando

$|P_{42} \cup P_{04} \cup P_{60}|$. Aplicamos la formula de inclusión y exclusión anterior:

$$\begin{aligned}|P_{42} \cup P_{04} \cup P_{60}| = &|P_{42}| + |P_{04}| + |P_{60}| \\ &- |P_{42} \cap P_{04}| - |P_{42} \cap P_{60}| - |P_{04} \cap P_{60}| \\ &+ |P_{42} \cap P_{04} \cap P_{60}|\end{aligned}$$

Contamos en primer lugar los elementos de P_{42}, de la manera siguiente: en todas las permutaciones que contienen "42"podemos agrupar el 4 y el 2 en un nuevo símbolo $\boxed{42}$. Esto define una biyección f de P_{42} en el conjunto de todas las permutaciones de $\{0, 1, 3, \boxed{42}, 5, 6, 7, 8, 9\}$. Por ejemplo:

$$f((9, 5, 1, 6, 0, 4, 2, 3, 8, 7)) = (9, 5, 1, 6, 0, \boxed{42}, 3, 8, 7)$$

Por lo tanto, P_{42} tiene 9! elementos.

Se procede similarmente con los otros 6 conjuntos: $P_{42} \cap P_{04}$ esta en biyección con las permutaciones de $\{\boxed{042}, 1, 3, 5, 6, 7, 8, 9\}$, $P_{42} \cap P_{60}$ esta en biyección con las permutaciones de $\{1, 3, \boxed{42}, 5, \boxed{60}, 7, 8, 9\}$, ...

Finalmente:

$$\begin{aligned}|P_{42} \cup P_{04} \cup P_{60}| = &\,9! + 9! + 9! \\ &- 8! - 8! - 8! \\ &+ 7!\end{aligned}$$

$\lozenge$

Enunciamos finalmente la formula en su versión más general.

Regla 8 (Principio de inclusión y exclusión). *Sean A_1, A_2, ..., A_n conjuntos. Entonces:*

$|A_1 \cup A_2 \cup \cdots \cup A_n| =$

la suma de los cardinales de los conjuntos

$-$ *la suma de los cardinales de las intersecciones dos por dos*

$+$ *la suma de los cardinales de las intersecciones tres por tres*

$-$ *la suma de los cardinales de las intersecciones cuatro por cuatro*

$\vdots$

3
Recursión

3.1 Introducción

Ejemplo 3.1.1.
Aquí esta un problema de combinatoria que las técnicas del Tema anterior no resuelven directamente: ¿ Cuántas son las cadenas de n bits sin ningún "00"(es decir sin ningún par de “0” consecutivos) ? Notamos a_n este numero. por lo tanto $a_0 = 1$ (para la cadena de longitud 0), y enumerando explícitamente las cadenas de n bits que cumplen la condición (ver cuadro 3.1) $a_1 = 2$, $a_2 = 3$, $a_3 = 5$, $a_4 = 8 \ldots$ ¿ Podemos obtener los valores de a_n más eficientemente ? ¿ Hay alguna formula general ? ¿ Podemos dar una buena aproximación de a_n para n grande ?

n	valor de a_n	cadenas de n bits sin ningún “00”
$n=1$	$a_1=2$	0 1
$n=2$	$a_2=3$	01 10 11
$n=3$	$a_3=5$	010 011 101 110 111
$n=4$	$a_4=8$	0101 0110 0111 1010 1011 1101 1110 1111
$\vdots$	$a_n=?$	$\cdots$

Cuadro 3.1: Cadenas de n bits sin ningún 00.

Para contestar observamos que si $n \geq 2$, cualquiera cadena de n bits sin ningún "00çumple una, y solamente una de las dos condiciones siguientes;

- o bien termina por 0. En este caso el penúltimo bit tiene que ser 1, y los bits anteriores pueden formar cualquiera cadena de longitud $n-2$ sin "00".
- o bien termina por “1”. En este caso, los bits anteriores pueden formar cualquiera cadena de longitud $n-1$ sin "00".

Cómo hay a_{n-1} cadenas de bits del primer tipo y a_{n-2} cadenas de bits del segundo tipo, obtenemos la relación:

$$a_n = a_{n-1} + a_{n-2} \qquad \text{para cualquier } n \geq 2$$

Esta relación es una *relación de recurrencia* para la sucesión $a_0, a_1, a_2 \ldots$: es una relación que expresa los términos de la sucesión en función de los términos con índices más pequeños. Gracias a esta relación, y los dos valores iniciales $a_0 = 1$ y $a_1 = 1$, podemos calcular eficientemente tantos valores a_n cómo queremos.

En este tema, estudiaremos cómo hallar una formula explicita para las sucesiones que cumplen ciertas relaciones de recurrencia. Obtendremos, por ejemplo, que la sucesión de los números a_n cumple:

$$a_n = \frac{1}{\sqrt{5}}\left(r_1^{n+1} - r_2^{n+1}\right)$$

donde r_1 y r_2 son las dos soluciones de la ecuación $x^2 = x + 1$. Más explícitamente, $r_1 = \frac{1+\sqrt{5}}{2}$ y $r_2 = \frac{1-\sqrt{5}}{2}$ (o *vice versa*), y por lo tanto:

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right)$$

Es satisfactorio obtener una tal expresión explicita. Obsérvese, sin embargo, que es de poca utilidad para calcular los un término particular a_n. Intente, por ejemplo, calcular a_{10} con esta formula. Es mucho más simple utilizar la relación de recurrencia.

Sin embargo la formula no es inútil: observamos que $|r_1| > 1$ y $|r_2| < 1$. Por lo tanto r_1^{n+1} tiene limite infinito y r_2^{n+1} tiene limite 0 para $n \to \infty$. Por lo tanto, estamos asegurados que $r_1^{n+1}/\sqrt{5}$ dará una buena aproximación de a_n para n grande (ver cuadro 3.2). Para $n = 10$ el error ya es más pequeño que 0,01 %. ♢

n	a_n	$r_1^{n+1}/\sqrt{5}$	error relativo
0	1	0,72	27 %
1	1	1,17	17 %
2	2	1,89	5,3 %
3	3	3,07	2,2 %
4	5	4,96	0,81 %
5	8	8,02	0,31 %
6	13	12,98	0,12 %
7	21	21,01	0,045 %
8	34	33,99	0,017 %
9	55	55,00	0,0066 %
10	89	89,00	0,0025 %

Cuadro 3.2: Error relativo cometido al aproximar a_n por $r_1^n/\sqrt{5}$

Más generalmente, una definición de una sucesión de objetos $f(0)$, $f(1)$, $f(2)$ … es *recursiva* cuando la definición de cada objeto (excepto los primeros) involucra los objetos anteriores.

Ejemplo 3.1.2. En matemáticas.
En matemáticas, la función *factorial* es la aplicación del conjunto de los enteros naturales en él mismo que asocia a n el producto de los n primeros enteros positivos. Una definición alternativa (pero equivalente) es la siguiente: es la función f del conjunto de los enteros naturales en él mismo que cumple: $f(0) = 1$ y, para cualquier $n > 0$, $f(n) = n \times f(n-1)$. Vemos que la definición de $f(n)$ (para $n \neq 0$) involucra $f(n-1)$. Esta definición del factorial es recursiva. ♢

Ejemplo 3.1.3. En programación.
Para calcular $n!$ podemos utilizar el algoritmo siguiente:

```
Factorial1(n):
  p ← 1
  Para i desde 1 hasta n:
     p ← p ∗ i
  Devolver p cómo resultado.
```

Otro algoritmo realizando el mismo trabajo es:

```
Factorial1(n):
  Si n = 0:
     Devolver 1 cómo resultado.
  Sino:
     Devolver n × FactorialRecursivo(n − 1) cómo resultado.
```

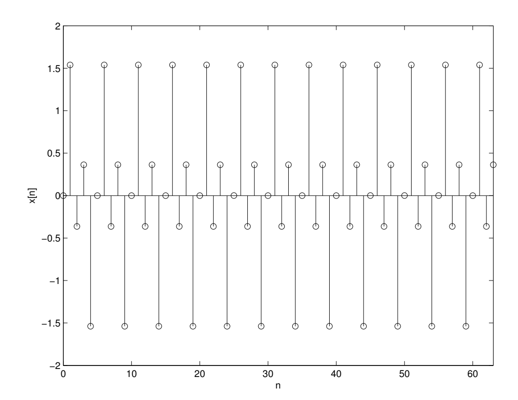
El segundo algoritmo es recursivo, el primero no lo es. ♢

Ejemplo 3.1.4.
En el ejemplo 3.1.1 tenemos una definición recursiva de la sucesión de los a_n. Consta de:

- la relación de recurrencia: $a_n = a_{n-1} + a_{n-2}, \qquad n \geq 0.$
- las *condiciones iniciales:* $a_0 = a_1 = 1$.

♢

En la sección 3.5 introduciremos también una técnica de demostración aparentada a la recursión: la *demostración por inducción*, que demuestra una sucesión infinita de proposiciones, utilizando que cada uno implica la siguiente.



$x[n] = \sin(2\pi f_1 n T_s) + \sin(2\pi f_2 n T_s)$, $f_1 = 1$ Hz, $f_2 = 2$ Hz, $f_s = 5$ Hz.

Figura 3.1: En tratamiento de la señal se consideran sucesiones cuyos índices son instantes sucesivos y cuyos términos son las medidas de una señal numérica discreta a estos instantes (Esta figura viene de una lección de tratamiento de la señal impartida en la ETSII).

3.2 *Sucesiones*

3.2.1 *Definiciones*

Definicion 3.2.1. *Una* sucesión numérica *se define especificando:*

- *un intervalo de enteros I,*
- *y asociando a cada elemento n de I un número.*

Los elementos de I se llaman los índices *de la sucesión, y los números asociados son los* términos *de la sucesión.*

Un intervalo de enteros es un conjunto de enteros consecutivos, cómo por ejemplo $\{1, 2, 3, 4, 5\}$, el conjunto de todos los números naturales $\mathbb{N}$, el conjunto de todos los enteros $\mathbb{Z}$ ...

En muchos contextos se consideran únicamente las sucesiones cuyo conjunto de índices es un intervalo de enteros de la forma $[p, +\infty)$ (todos los enteros superiores o igual a p). Será el caso en esta lección.

En general para nombrar la sucesión, se suele utilizar una letra (por ejemplo a). Entonces el término de índice n lo notamos a_n (o sea, el término de índice 1 es a_1, el término de índice 2 es a_2 ...).. Nos podemos referir a la sucesión por su nombre: a, o utilizando la notación siguiente: $(a_n)_{n\in I}$, que se lee: "la sucesión de los a_n para n en I. Si I es un intervalo de enteros de la forma $[p, +\infty)$ se suele notar también: $(a_n)_{n\geq p}$.

No es prohibido notar $a(n)$ los términos de la sucesión. A veces, al contrario, es conveniente.

Ejemplo 3.2.1.
Hay una sucesión cuyos índices son los números naturales, tal que el término de índice n es n^2. Sus primeros términos aparecen en el cuadro 3.2.

Si llamamos b esta sucesión, tenemos $b_0 = 0$, $b_1 = 1$, $b_2 = 4$ ... y en general $b_n = n^2$ para cualquier $n \geq 0$. Podemos referirnos a la sucesión b cómo $(n^2)_{n\in\mathbb{N}}$ cómo $(n^2)_{n\geq 0}$, o cómo $(b_n)_{n\geq 0}$. ♢

Índice n	0	1	2	3	4	...
Término n^2	0	1	4	9	16	...

Figura 3.2: Los primeros términos de la sucesión de los cuadrados de los enteros naturales.

Podemos hacer operaciones con sucesiones:

- la suma de dos sucesiones con el mismo conjunto de índices. Si las dos sucesiones son $u = (u_n)_{n\in I}$ y $v = (v_n)_{n\in I}$ entonces su suma es $u + v = (u_n + v_n)_{n\in I}$.
- También, podemos multiplicar una sucesión por un número: el producto de $u = (u_n)_{n\in I}$ por el número x es $x \cdot u = (xu_n)_{n\in I}$.

Son las misma reglas que para la suma de vectores: $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$, excepto que aquí los vectores son "de longitud infinita".

Las sucesiones de números reales (o complejos) con conjunto de índices I forma un espacio vectorial, ver el curso de álgebra lineal impartido al segundo cuatrimestre.

Ejemplo 3.2.2.
Si $u = (n^2)_{n\geq 1}$ (es decir, para cualquier $n \geq 1$, $u_n = n^2$) y $v = (2\,n + 1)_{n\geq 1}$ (para cualquier $n \geq 1$, $v_n = 2\,n+1$) entonces $u + v = (n^2 + 2\,n + 1)_{n\geq 1}$. ♢

Definicion 3.2.2. *Una* combinación lineal *de sucesiones u, v, w ... es cualquiera sucesión de la forma $x\,u + y\,v + z\,w + \cdots$ con $x, y, z, \ldots$ números. O sea: es una suma con coeficientes de las sucesiones.*

Ejemplo 3.2.3.
Si $u = (n^2)_{n\geq 1}$ y $v = (2\,n+1)_{n\geq 1}$ entonces $(-n^2 + 4\,n + 2)_{n\geq 1}$ es una combinación lineal de u y v. En efecto, es $-u + 2\,v$. ♢

Cuando disponemos de una formula para los términos u_n de una sucesión, en función del índice n, nos referimos a esta formula cómo *el término general* de la sucesión.

Ejemplo 3.2.4.
La "sucesión de término general n^2" con conjunto de índices $\mathbb{N}$ es la sucesión $(n^2)_{n\geq 0}$, es decir la sucesión u tal que $u_n = n^2$ para cualquier $n \geq 0$. ♢

Podemos también hacer cambios de índices (análogos a los cambios de variable de una función).

Ejemplo 3.2.5.
Sea b la sucesión de los cuadrados de los enteros naturales, es decir $b = (n^2)_{n\geq 0}$. Entonces la sucesión $c = (b_{n+1})_{n\geq 0}$ es una nueva sucesión, cuyos primeros términos son $c_0 = b_1 = 1$, $c_1 = b_2 = 4$, $c_2 = b_3 = 9 \ldots$
♢

Ejemplo 3.2.6.
Sea u la sucesión de término general n^2 y cuyos índices están en $\mathbb{N}$. Es decir $u = (n^2)_{n\geq 0}$. Sea v la sucesión de término general $u_{n+2} - u_{n+1} - u_n$, y conjunto de índices $\mathbb{N}$. Entonces para cualquier $n \geq 0$:

$$v_n = (n+2)^2 - (n+1)^2 - n^2 = (n^2 + 4n + 4) - (n^2 + 2n + 1) - n^2$$

Reagrupamos los términos en n^2, los términos en n y los términos constantes:

$$v_n = (1 - 1 - 1)n^2 + (4 - 2)n + (4 - 1) = -n^2 + 2n + 3$$

Por lo tanto, v es la sucesión de término general $-n^2 + 2n + 3$. ♢

3.3 *Ecuaciones de recurrencia*

3.3.1 *Definiciones*

Hemos visto (ya en el ejemplo **??**) que ciertas sucesiones satisfacen relaciones de recurrencia. Podemos también empezar con una relación de recurrencia, y buscar todas las sucesiones que la satisfacen. Hablamos, en este caso, de *ecuación de recurrencia*.

Ejemplo 3.3.1.

$$u_{n+1} = 2\,u_n, \text{ para cualquier } n \geq 0$$

es una ecuación de recurrencia. No es difícil resolverla: sus soluciones son exactamente la sucesión $(2^n)_{n\geq 0}$ y todos sus múltiplos. ♢

Estudiaremos métodos de resolución de ciertos tipos de ecuación de recurrencia solamente, que forman parte de las *ecuaciones de recurrencia lineales a coeficientes constantes*.

Definicion 3.3.1. *Una ecuación de recurrencia lineal a coeficientes constantes es una ecuación de recurrencia que puede ponerse de la forma:*

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} + g(n) \qquad \textit{para cualquier } n \geq p \quad (3.1)$$

dónde:

- *p es un entero.*
- *k es un entero positivo, llamado* orden *de la ecuación.*
- *$a_0, a_1, \ldots, a_{k-1}$ son números. Son los* coeficientes *de la ecuación.*
- *g es una sucesión con índices $n \geq p$, llamada* término independiente *de la ecuación.*

Además, si $g = 0$, decimos que la ecuación de recurrencia lineal es homogénea.

Ejemplo 3.3.2.
La ecuación de recurrencia:

$$u_{n+2} = u_{n+1} + u_n + n^2, \qquad \text{para cualquier } n \geq 0$$

es lineal a coeficientes constantes. Su orden es $k = 2$, sus coeficientes son $a_0 = a_1 = 1$, su término independiente es $g(n) = n^2$. Cómo $g(n) \neq 0$, no es homogénea. ♢

Ejemplo 3.3.3.
La ecuación de recurrencia:

$$u_n = u_{n-1} + u_{n-2} + n^2, \qquad \text{para cualquier } n \geq 2$$

no es exactamente de la forma (3.10). Sin embargo, podemos hacer una "cambio de índices" (cómo un cambio de variables), poniendo $m = n - 2$ (y por lo tanto $n = m + 2$). La ecuación de recurrencia es equivalente a:

$$u_{m+2} = u_{m+1} + u_m + (m+2)^2, \qquad \text{para cualquier } m \geq 0$$

(Obsérvese que $n \geq 2$ es equivalente a $m \geq 0$ ya que $m = n - 2$). Si queremos, podemos utilizar otra vez n cómo variable (ya que es una "variable muda"). Obtenemos la ecuación de recurrencia equivalente:

$$u_{n+2} = u_{n+1} + u_n + (n+2)^2, \qquad \text{para cualquier } m \geq 0$$

♢

Ejemplo 3.3.4.
Las ecuaciones de recurrencia siguientes no son lineales a coeficientes constantes:

- $u_{n+1} = u_n^2$.
- $u_{n+1} = (n+1)\, u_n$. (el coeficiente $n+1$ no es constante, varia cuando n varia).
- $u_{n+1} = u_n + u_{n-1} + u_{n-2} + \cdots + u_1 + u_0$.

◊

3.3.2 *Un poco de álgebra lineal*

A continuación desarrollamos en un ejemplo una analogía entre, por una parte, las sucesiones y las ecuaciones de recurrencia lineales a coeficientes constantes, y, por otra parte, los vectores y los sistemas de ecuaciones lineales. De hecho, es más que una analogía: son dos casos particulares de una misma teoría general (el álgebra lineal). Pero para descubrir esta teoría en toda su generalidad, los estudiantes de IS tendrán que esperar el segundo cuatrimestre.

Ecuaciones lineales.

Esto es una ecuación lineal:

$$x + y + z = 1 \tag{3.2}$$

Sus incógnitas son x, y, z. Podemos decir también que consideramos un vector incógnito (x, y, z). El conjunto de las soluciones del sistema es un subconjunto de $\mathbb{R}^3$ (de hecho es una plano). Contiene, por ejemplo, el vector $(1, -1, 1)$.

Esto es una ecuación de recurrencia lineal:

$$u_{n+2} - u_{n+1} - u_n = 3^n, \qquad n \geq 0 \tag{3.3}$$

Representa una sistema de (un número infinito de) ecuaciones, cada una correspondiendo a un valor de n:

$$\left\{ \begin{aligned} u_2 - u_1 - u_0 &= 1 \\ u_3 - u_2 - u_1 &= 3 \\ u_4 - u_3 - u_2 &= 9 \\ &\vdots \end{aligned} \right. \tag{3.4}$$

Hay un numero infinito de incógnitas, son $u_0, u_1, u_2 \ldots$ Podemos decir también que tenemos una sucesión incógnita u. El conjunto de las soluciones es un subconjunto del espacio de las sucesiones numéricas con índices en $\mathbb{N}$. Contiene, por ejemplo, la sucesión $(3^n/5)_{n\geq 0}v$.

El conjunto de las soluciones y la "solución general".

Resolviendo la ecuación (3.2), obtenemos otra descripción del conjunto de sus soluciones: es el conjunto de todos los vectores de la forma $(1-s-t, s, t)$ para s, $t \in \mathbb{R}$. Por ejemplo, el vector solución $(1, -1, 1)$ se obtiene con -1 y $t = 1$. Eligiendo $s = t = 0$ obtenemos otra solución: $(1, 0, 0)$. Decimos que $(1-s-t, s, t)$ es la solución general del sistema: significa que es una formula que da todas las soluciones. En esta formula, s y t son parámetros.

A continuación, presentaremos técnicas que nos permiten resolver la ecuación de recurrencia (3.3). Obtendremos que el conjunto de las soluciones es el conjunto de todas las sucesiones de la forma $(s\,r_1^n + t\,r_2^n + 3^n/5)_{n\geq 0}$ para s y t en $\mathbb{R}$, donde r_1 y r_2 son las dos soluciones de la ecuación $x^2 - x - 1 = 0$ (valen, por lo tanto, $(1+\sqrt{5})/2$ y $(1-\sqrt{5})/2$). Por ejemplo, eligiendo $s = t = 0$ obtenemos la solución $(3^n/5)$. Eligiendo $s = 1$ y $t = 0$ obtenemos otra solución: $(r_1^n + 3^n/5)_{n\geq 0}$. Decimos que $(s\,r_1^n + t\,r_2^n + 3^n/5)_{n\geq 0}$ es la solución general de la ecuación de recurrencia, con parámetros s y t.

Definicion 3.3.2. *Llamamos "solución general" de una ecuación de recurrencia lineal a coeficientes constantes una formula para el término general de la sucesión, que depende de parámetros.*

La ecuación homogénea asociada.

Esto es la *ecuación homogénea asociada a la ecuación* (3.2):

$$x + y + z = 0$$

Se obtiene de la ecuación (3.2) cancelando los "términos constantes" (los que no vienen en factor de ninguna incógnita). Su conjunto de soluciones también es un subconjunto de $\mathbb{R}^3$. Necesariamente contiene el vector 0 de $\mathbb{R}^3$ (es decir, el vector $(0, 0, 0)$).

Esto es la *ecuación de recurrencia lineal homogénea asociada a* (3.3)):

$$u_{n+2} - u_{n+1} - u_n = 0, \qquad n \geq 0$$

Se obtiene de (3.3) cancelando todos los términos que no vienen en factor de ninguna incógnita u_k. Su conjunto de soluciones también es un conjunto de soluciones. Necesariamente contiene la sucesión 0 (es decir la sucesión z definida por: $z_n = 0$ para cualquier $n \geq 0$).

Definicion 3.3.3. *Recordamos la ecuación de recurrencia lineal a coeficientes constantes* (3.10)*:*

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} + g(n) \quad \text{para cualquier } n \geq p$$

La ecuación de recurrencia homogénea asociada es la ecuación obtenida sus-

tituyendo $g(n)$ por 0. Es:

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} \quad \textit{para cualquier } n \geq p$$

La solución general de una ecuación homogénea.

La solución general de la ecuación homogénea asociada a (3.2) es: $(-s-t, s, t)$. Se descompone en: $s\ (-1,1,0) + t\ (-1,0,1)$. Por lo tanto, el plano de las soluciones de esta ecuación homogénea es exactamente el conjunto de todas las combinaciones lineales de $(-1,1,0)$ y de $(-1,0,1)$ (decimos que estos dos vectores forman una base del plan).

La solución general de la ecuación de recurrencia homogénea asociada a (3.3) es: $(s\, r_1^n + t\, r_2^n)_{n\geq 0}$. Se descompone en: $s\ v + t\ w$, donde $v = (r_1^n)_{n\geq 0}$ y $w = (r_2^n)_{n\geq 0}$. Por lo tanto, el conjunto de las soluciones de la ecuación de recurrencia homogénea asociada a (3.3) es exactamente el conjunto de todas las combinaciones lineales de las dos sucesiones v y w (diremos que estas dos sucesiones forman una base del espacio de las soluciones).

Para las ecuaciones de recurrencia lineales homogéneas a coeficientes constantes, tenemos el resultado siguiente (que no demostraremos).

Teorema 3.3.4. *El conjunto de las soluciones de una ecuación de recurrencia lineal homogénea a coeficientes constantes de orden k es siempre el conjunto de las combinaciones lineales de ciertas k soluciones. Del conjunto de estas k soluciones, diremos que es una* base *de las soluciones.*

Ejemplo 3.3.5.
Para la ecuación de recurrencia homogénea asociada a (3.3), las sucesiones $v = (r_1^n)_{n\geq 0}$ y $w = (r_2^n)_{n\geq 0}$ forman una base de soluciones. ♢

Obsérvese que si una base de soluciones de la ecuación de recurrencia homogénea es $\{f_1, f_2, \ldots, f_k\}$ (cada f_i es una sucesión), entonces su solución general es $t_1 f_1 + t_2 f_2 + \cdots + t_k f_k$, con t_1, t_2, …, t_k parámetros.

La solución general de una ecuación, y la solución general de la ecuación homogénea asociada

La solución de la ecuación homogénea asociada a (3.2) se obtiene de la solución general de (3.2) cancelando los términos constantes. Recíprocamente, tenemos la descomposición: $(1-s-t, s, t) = (1{,}0{,}0) + (-s-t, s, t)$ que interpretamos así: la solución general de la ecuación (3.2) es la suma de una solución particular de (3.2) y de la solución general de su ecuación homogénea asociada.

La solución general de la ecuación de recurrencia homogénea asociada a (3.3) se obtiene de la solución general de (3.3) cancelando los términos constantes. Recíprocamente, tenemos la descomposición: $(s\, r_1^n + t\, r_2^n + 3^n/5)_{n\geq 0} = (3^n/5)_{n\geq 0} + (s\, r_1^n + t\, r_2^n)_{n\geq 0}$ que interpretamos así: la solución general de la ecuación de recurrencia (3.3) es la suma de una solución particular de (3.3) y de la solución general de su ecuación de recurrencia homogénea asociada.

Tenemos el resultado general siguiente:

Teorema 3.3.5. *La solución general de una ecuación de recurrencia lineal a coeficientes constantes es la suma de una solución particular suya (cualquiera) y de la solución general de la ecuación de recurrencia homogénea asociada.*

Es fácil dar una demostración.

Demostración. La ecuación de recurrencia es de la forma:

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} + g(n) \quad \text{para cualquier } n \geq p \tag{3.5}$$

Sea v una solución cualquiera de esta ecuación. Significa que se cumple:

$$v_{n+k} = a_0 v_n + a_1 v_{n+1} + a_2 v_{n+2} + \cdots + a_{k-1} v_{n+k-1} + g(n) \quad \text{para cualquier } n \geq p \tag{3.6}$$

Para n fijo, las dos ecuaciones (de incógnitas $w_n, w_{n+1}, \ldots, w_{n+k}$):

$$(w_{n+k} + v_{n+k}) = a_0(w_n + v_n) + a_1(w_{n+1} + v_{n+1)} + a_2(w_{n+2} + v_{n+2)} + \cdots + a_{k-1}(w_{n+k-1} + v_{n+1)}$$

y

$$w_{n+k} = a_0 w_n + a_1 w_{n+1} + a_2 w_{n+2} + \cdots + a_{k-1} w_{n+k-1} + g(n) \tag{3.7}$$

son equivalentes ya que cada una se obtiene de la otra añadiendo o sustrayendo término a término la igualdad:

$$v_{n+k} = a_0 v_n + a_1 v_{n+1} + a_2 v_{n+2} + \cdots + a_{k-1} v_{n+k-1} + g(n)$$

De esto deducimos que w es solución de la ecuación homogénea asociada a (3.5) si y solo si $w + v$ es solución de (3.5). □

3.4 Recetas para resolver la ecuaciones de recurrencia lineales a coeficientes constantes, homogéneas o con término constante casi–polinomial

Resolver una ecuación de recurrencia lineal a coeficientes constantes significa: dar una formula para su solución general. Vamos a presentar una receta para resolver un pequeña, aunque importante, clase de ecuaciones de recurrencia lineales a coeficientes constantes. Son las ecuaciones

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} + r^n P(n) \quad \text{para cualquier } n \geq p \tag{3.8}$$

con P polinomio (es decir: $P(n) = c_0 + c_1 n + c_2 n^2 + \cdots + c_d n^d$). Es decir, son las ecuaciones de recurrencia lineales a coeficientes constantes cuyo término independiente es el producto de una sucesión exponencial r^n y de una sucesión polinomial $P(n)$. Incluye (con $P = 0$) la clase de las ecuaciones de recurrencia lineales *homogéneas* a coeficientes constantes.

3.4.1 método general

La receta se basa sobre el teorema 3.3.5, que dice que la solución general de (3.8) es la suma de una solución particular de (3.8) y de la solución general de la ecuación homogénea asociada. La receta consiste, por lo tanto, en:

1. Resolver la ecuación homogénea asociada.
2. Hallar una solución particular de (3.8).
3. Hacer la suma.

3.4.2 Resolución de la ecuación de recurrencia lineal homogénea a coeficientes constantes

Consideramos la ecuación de recurrencia lineal homogénea a coeficientes constantes:

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} \quad \text{para cualquier } n \geq p \tag{3.9}$$

Definicion 3.4.1. *La* ecuación característica *de una ecuación de recurrencia lineal homogénea a coeficientes constantes* (3.9) *es la ecuación obtenida cambiando cada u_{n+i} por x^i (es decir: u_{n+k} por x^k, u_{n+k-1} por x^{k-1}, ..., u_{n+1} por x^1, que vale x, u_n por x^0, que vale 1). Es, por lo tanto:*

$$x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{3.10}$$

Ejemplo 3.4.1.
La ecuación característica de:

$$u_{n+2} = u_{n+1} + u_n, \qquad \text{para cualquier } n \geq 0$$

es $x^2 = x + 1$ (obtenida sustituyendo u_{n+2} por x^2, u_{n+1} por x^1, que vale x, y u_n por x^0, que vale 1). $\diamondsuit$

Enunciamos ya el teorema que proporciona la solución general de (3.9).

Teorema 3.4.2. *Sean $r_1, r_2, \ldots, r_s$ todas las soluciones de la ecuación característica de (3.9), y $m_1, m_2, \ldots, m_s$ sus multiplicidades respectivas. Entonces una base de soluciones de (3.9) es:*

$$\begin{array}{ccccc} (r_1^n) & (n\, r_1^n) & (n^2\, r_1^n) & \cdots & (n^{m_1-1}\, r_1^n) \\ (r_2^n) & (n\, r_2^n) & (n^2\, r_2^n) & \cdots & (n^{m_2-1}\, r_2^n) \\ \vdots & & \vdots & & \vdots \\ (r_s^n) & (n\, r_s^n) & (n^2\, r_s^n) & \cdots & (n^{m_s-1}\, r_s^n) \end{array}$$

Recordamos lo que son las multiplicidades de las raíces de una ecuación polinomial. La ecuación:

$$x^k = a_0 + a_1\, x + \cdots + a_{k-1} x^{k-1}$$

es equivalente a

$$P(x) = 0$$

donde $P(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0$. Es un polinomio de grado k.

Teorema 3.4.3. *Un polinomio $P(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0$ admite una factorización de la forma:*

$$(x - r_1)^{m_1}(x - r_2)^{m_2} \cdots (x - r_s)^{m_s}$$

donde los r_i son números complejos (reales o imaginarios) y los m_i son números estrictamente positivos. Además esta factorización es única, excepto por el orden de los factores $(x - r_i)^{m_i}$.

Cómo consecuencia, vemos que $r_1, r_2, \ldots, r_s$ son exactamente las soluciones (o "raíces") de $P(x) = 0$. El entero m_i se llama multiplicidad de la solución *r_i.*

Obsérvese que la suma de las multiplicidades m_i es igual a k, el grado de P.

Ejemplo 3.4.2.

- El polinomio $x^3 - x^2 - x + 1$ se factoriza cómo: $(x-1)^2(x+1)$. Tiene, por lo tanto, dos raíces: la raíz 1, que tiene multiplicidad 2, y la raíz -1, que tiene multiplicidad 1.
- El polinomio $x^4 - 1$ se factoriza cómo $(x-1)(x-i)(x+1)(x+i)$, dónde i es una raíz cuadrada de -1 (es un número complejo imaginario). Por lo tanto tiene cuatro raíces, todas de multiplicidad 1.

$\Diamond$

Ejemplo 3.4.3.
Cuando todas las soluciones de la ecuación característica son simples entonces son $s = k$ soluciones y el término general de la solución general de (3.9) es:

$$t_1 r_1^n + t_2 r_2^n + \cdots + t_k r_k^n$$

$\Diamond$

Una solución es *simple* cuando tiene multiplicidad $m = 1$.

Ejemplo 3.4.4.
Consideramos la ecuación de recurrencia:

$$u_{n+2} = u_{n+1} + u_n$$

Su ecuación característica es:

$$x^2 = x + 1$$

Es equivalente a $P(x) = 0$ con $P(x) = x^2 - x - 1$. La ecuación tiene dos soluciones distintas r_1 y r_2, necesariamente simples (ya que m_1 y m_2 cumplen $m_1 + m_2 = 2$ y $m_1 > 0$, $m_2 > 0$). Por lo tanto el conjunto de las soluciones de la ecuación de recurrencia admite como base el conjunto formado de $(r_1^n)_{n\geq 0}$ y $(r_2^n)_{n\geq 0}$. Por lo tanto, la solución general de la ecuación de recurrencia tiene término general:

$$s\, r_1^n + t\, r_2^n$$

con s y t parámetros. $\Diamond$

Ejemplo 3.4.5.
Consideramos la ecuación de recurrencia:

$$u_{n+2} = 4\, u_{n+1} - 4\, u_n$$

Su ecuación característica es:

$$x^2 = 2\, x - 4$$

Es equivalente a $P(x) = 0$ con $P(x) = x^2 - 4\, x + 4$. Factorizamos fácilmente P, es igual a $(x-2)^2$. Por lo tanto $P(x) = 0$ tiene una única solución, es $x = 2$, y esta solución tiene multiplicidad $m = 2$. El conjunto de las soluciones de la ecuación de recurrencia admite como base el conjunto formado por $(2^n)_{n\geq 0}$ y $(n\, 2^n)_{n\geq 0}$. Finalmente la solución general de la ecuación de recurrencia tiene término general:

$$t_0\, 2^n + t_1\, n\, 2^n.$$

con t_0 y t_1 parámetros. $\Diamond$

Ejemplo 3.4.6.
Consideramos la ecuación de recurrencia:

$$u_{n+4} = 2\, u_{n+2} - u_n$$

Su ecuación característica es:

$$x^4 = 2\, x^2 - 1$$

Es equivalente a $P(x) = 0$ con $P(x) = x^4 - 2x^2 + 1$. Factorizamos fácilmente P, es igual a $(x^2-1)^2 = (x-1)^2(x+1)^2$. Por lo tanto $P(x) = 0$ tiene dos soluciones, son $x = 1$ y $x = -1$, y cada una tiene multiplicidad 2. Por lo tanto, el conjunto de las soluciones de la ecuación de recurrencia admite cómo base el conjunto formado de las sucesiones: $((-1)^n)_{n\geq 0}$, $(n\,(-1)^n)_{n\geq 0}$, $(1)_{n\geq 0}$, $(n)_{n\geq 0}$. La solución general tiene término general

$$(-1)^n\, t_1 + n\,(-1)^n t_2 + t_3 + n\, t_4$$

con t_1, t_2, t_2, t_4 parámetros. ♢

3.4.3 *Una receta para hallar una solución particular de* (3.8)

Se basa en el teorema siguiente, que no demostraremos.

Teorema 3.4.4. *Consideramos la ecuación*

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} + r^n P(n) \quad \text{para cualquier } n \geq p \qquad (3.8)$$

con P polinomio de grado d. Sea m la multiplicidad de r cómo raíz de la ecuación característica de la ecuación homogénea asociada a (3.8) *(si r no es raíz de la ecuación característica, entonces la multiplicidad m vale* 0*). Entonces* (3.8) *admite una única solución de la forma $(r^n n^m Q(n))_{n\geq p}$ con Q polinomio de grado d.*

Para encontrar la solución cuya existencia viene asegurada por el teorema 3.4.4, escribimos Q con coeficientes indeterminados:

$$Q(n) = c_0 + c_1 n + c_2 n^2 + \cdots + c_d n^d$$

y ponemos $u_n = r^n n^m Q(n)$. Inyectamos esta expresión en la ecuación de recurrencia y reagrupamos los términos según las potencias de n. Nos queda a resolver un sistema lineal de ecuaciones en las $d+1$ variables c_0, c_1, $\ldots$, c_d que, según el teorema, tiene una solución única.

Ejemplo 3.4.7.
Resolvemos la ecuación de recurrencia:

$$u_{n+1} = 2\, u_n + 3 \text{ para cualquier } n \geq 0. \qquad (3.11)$$

Resolvemos en primer lugar la ecuación de recurrencia homogénea asociada. Es inmediato obtener su solución general: es la sucesión de término general $t\ 2^n$, donde t es un parámetro. Buscamos ahora una solución particular de la ecuación completa. Cómo su término independiente es $g(n) = 3$, que podemos escribir cómo 3×1^n. Es de la forma $r^n P(n)$, con $r = 1$ y $P(n) = 3$ (grado $d = 0$). Cómo 1 no es raíz de la ecuación característica de la ecuación homogénea asociada a (3.11), su multiplicidad es $m = 0$ (la ecuación característica es $x = 2$). Buscamos la única solución de (3.11) de la forma $u = (1^n n^0 Q(n))$ con Q de grado 0, es decir: $Q(n) = c_0$ (una constante).

Sustituyendo u_n y u_{n+1} por c_0 en la ecuación de recurrencia, obtenemos la condición:

$$c_0 = 2\,c_0 + 3 \text{ para cualquier } n \geq 0.$$

Esta condición se simplifica en $c_0 = -3$. Concluimos que la sucesión constante de término general -3 es una solución particular de la ecuación completa. Aplicando el teorema, obtenemos que la solución general de la ecuación de recurrencia es la sucesión de término general $2^n - 3$. ♢

Ejemplo 3.4.8.
Vamos a obtener la solución general de:

$$u_{n+2} = 2\,u_{n+1} - u_n + n^2 \text{ para cualquier } n \geq 0. \tag{3.12}$$

Hemos obtenido la solución de la ecuación homogénea asociada en el ejemplo **??**: es la sucesión de término general $t_0 + nt_1$. La ecuación característica es $x^2 = 2\,x - 1$, equivalente a $(x-1)^2 = 0$. El término independiente de (3.12) es (n^2), de la forma $(r^n P(n))$ con $r = 1$ y $P(n) = n^2$ (grado $d = 2$). Cómo r es raíz doble (= de multiplicidad $m = 2$) de la ecuación característica, buscamos la única solución de (3.12) de la forma $(1^n n^2 Q(n))$ con Q de grado 2, o sea: $u_n = n^2 Q(n) = en^4 + dn^3 + an^2$. Calculamos:

$$\begin{aligned} u_{n+1} &= e(n+1)^4 + d(n+1)^3 + a(n+1)^2 \\ &= en^4 + (d+4e)n^3 + (a+3d+6e)n^2 + \\ &\qquad (2a+3d+4e)n + (a+d+e) \end{aligned}$$

y

$$\begin{aligned} u_{n+2} &= e(n+2)^4 + d(n+2)^3 + a(n+2)^2 \\ &= en^4 + (d+8e)n^3 + (a+6d+24e)n^2 + \\ &\qquad (4a+12d+32e)n + (4a+8d+16e) \end{aligned}$$

Nos conduce al sistema:

$$\begin{cases} e = 2e - e \\ d + 8e = 2(d+4e) - d \\ a + 6d + 24e = 2(a+3d+6e) - a + 1 \\ 4a + 12d + 32e = 2(2a+3d+4e) \\ 4a + 8d + 16e = 2(a+d+e) \end{cases}$$

Es equivalente a:

$$\begin{cases} 0 = 0 \\ 0 = 0 \\ 12e = 1 \\ d + 4e = 0 \\ a + 3d + 7e = 0 \end{cases}$$

Su única solución es: $a = 5/12$, $d = -4/12$, $e = 1/12$. Corresponde a la solución particular de término general $\frac{1}{12}(n^4 - 4n^3 + 5n^2)$ de la ecuación de recurrencia.

Por lo tanto, la solución general de la ecuación de recurrencia es la sucesión de término general:

$$\frac{1}{12}(n^4 - 4n^3 + 5n^2) + t_1 n + t_0$$

con t_0 y t_1 parámetros. ♢

3.5 *Demostraciones por inducción*

3.5.1 *Inducción simple*

La *inducción matemática* es una técnica de demostración que sirve para demostrar una sucesión, posiblemente infinita, de proposiciones, por ejemplo:

Inducción tiene un sentido diferente en otras áreas.

> "Para cualquier entero n positivo, la suma de los n primeros enteros positivos vale $n(n+1)/2$"

que resume la sucesión infinita de proposiciones:

$$\begin{array}{rcl} 1 & = & 1 \\ 1+2 & = & 2\times 3/2 \\ 1+2+3 & = & 3\times 4/2 \\ 1+2+3+4 & = & 4\times 5/2 \\ & \vdots & \end{array}$$

Se acepta cómo demostración válida de todas las proposiciones de la sucesión la demostración de las dos proposiciones siguientes:

1. La demostración de la primera de las proposiciones ("caso base").
2. La demostración del hecho que cada una de las proposiciones implica la siguiente.

La idea es simple. Con un ejemplo de la vida cotidiana: si una ley estipula que este año tengo que llenar una declaración de renta, y otra ley estipula que cada persona que llena una declaración de renta algún año, tendrá que llenar también una declaración de renta el año siguiente, entonces, según la ley, tendré que llenar una declaración de renta cada año a partir de este.

Ejemplo 3.5.1.
Vamos a demostrar por inducción que para cualquier entero n positivo, la suma de los n primeros enteros positivos vale $n(n+1)/2$.

Demostración

Para cualquier entero positivo n, llamamos $P(n)$ la proposición:

> "La suma de los n primeros enteros positivos vale $n(n+1)/2$"

Comentarios

Damos un nombre a las proposiciones. No es obligatorio, pero es cómodo. Aquí, por ejemplo. $P(3)$ es la proposición: "La suma de los 3 primeros enteros positivos vale $3\times 4/2$."

Demostramos en primer lugar $P(1)$. Esta proposición dice:

> "La suma de los 1 primeros enteros positivos vale $1\times 2/2$"

Es el primer paso de la demostración: demostramos el "caso base".

Es cierta, ya que $1\times 2/2 = 1$. Por lo tanto $P(1)$ queda demostrada.

Ahora fijamos $n > 0$ y suponemos (por un momento) que $P(n)$ es cierta, es decir que:

$$1+2+\ldots+n = n(n+1)/2$$

Añadimos $n+1$ en ambos lados de la igualdad:

$$1+2+\ldots+n+(n+1) = n(n+1)/2+(n+1)$$

Observamos (factorizando por $n+1$) que $n(n+1)/2+(n+1) = (n/2+1)(n+1) = (n+2)/2\times(n+1) = (n+1)(n+2)/2$. Por lo tanto:

$$1+2+\ldots+n+(n+1) = (n+1)(n+2)/2.$$

Es decir, $P(n+1)$ es cierta.

El segundo paso de la demostración por inducción consiste en demostrar que para cualquier n positivo, $P(n) \Rightarrow P(n+1)$. Se hace fijando n arbitrario (de manera que la demostración de la implicación $P(n) \Rightarrow P(n+1)$ funcione para todos los n a la vez), suponiendo por un momento $P(n)$ cierta, y deduciendo bajo esta hipótesis que $P(n+1)$ sería cierta también.

(Aclaración: este "$P(n+1)$ es cierta" vale bajo la hipótesis "$P(n)$ cierta").

En fin, acabamos de demostrar que para cualquier $n > 0$, $P(n)$ implica $P(n+1)$, y hemos comprobado anteriormente que $P(1)$ es cierta. Por inducción, podemos concluir que $P(n)$ es cierta para cualquier $n > 0$.

Esta frase de conclusión es importante. Estudiantes, tenéis que escribirla (o alguna frase equivalente).

◊

Ejemplo 3.5.2.
Vamos a demostrar por inducción que $n! > 2^n$ para todos los enteros positivos n "suficientemente grande". Calculamos en primer lugar los primeros valores de estas cantidades.

n	1	2	3	4	5	6
$n!$	1	2	6	24	120	720
2^n	2	4	8	16	32	54

A partir de estas observaciones (en particular viendo cómo $n!$ parece crecer tantas veces más rápidamente que 2^n) adivinamos que tendremos $n! > 2^n$ para cualquier $n \geq 4$. Es lo que vamos a demostrar por inducción. La hipótesis de inducción será:

$P(n)$: " $n! > 2^n$"

Demostramos en primer lugar el caso base. Aquí es $P(4)$. Por cálculo directo, $P(4)$ es cierta.

Luego demostramos que para cualquier $n \geq 4$, $P(n)$ implica $P(n+1)$. Fijamos $n \geq 4$ y suponemos $P(n)$ cierta, es decir, $n! > 2^n$. Para hacer aparecer $(n+1)!$, multiplicamos ambos lados de la desigualdad por $n+1$. Obtenemos $(n+1)! > (n+1)2^n$. Cómo $n \geq 4$, tenemos $n + 1 \geq 2$ (no necesitamos más). Por lo tanto, $(n+1)2^n > 2 \cdot 2^n = 2^{n+1}$. Deducimos que $(n+1)! > 2^{n+1}$, es decir que $P(n+1)$ es cierta.

Acabamos de demostrar que para cualquier $n \geq 4$, $P(n)$ implica $P(n+1)$. Habíamos comprobado anteriormente que $P(4)$ es cierta. Por inducción, concluimos que $P(n)$ es cierta para cualquier n. ◊

A veces no es inmediato encontrar "la buena" hipótesis de recurrencia.

Ejemplo 3.5.3.
¿ Cuales son los enteros podemos obtener como sumas de 3 y de 8 (con repeticiones) ?

$$\begin{aligned}
3 &= 3 \\
6 &= 3+3 \\
8 &= 8 \\
9 &= 3+3+3 \\
11 &= 8+3 \\
12 &= 3+3+3+3 \\
14 &= 3+3+8 \\
15 &= 3+3+3+3+3 \\
16 &= 8+8 \\
&\vdots
\end{aligned}$$

y parece que a partir de 14 podemos obtenerlos todos. Vamos a demostrarlo por inducción.

Para cualquier n positivo, sea $P(n)$ la proposición:

"el número n es una suma de 3 y de 8"

Queremos demostrar que $P(n)$ es cierto para todo $n \geq 14$.

Para demostrar el caso base $P(14)$ basta exhibir la descomposición:

$$14 = 8 + 3 + 3$$

Queremos demostrar ahora que para cualquier $n \geq 14$, si $P(n)$ es cierta entonces $P(n+1)$ es cierta también. Escribimos:

$$n + 1 = (n - 2) + 3$$

y vemos que la hipótesis $P(n)$ no sirve aquí. Lo que serviría sería $P(n-2)\ldots$

Lo arreglamos todo introduciendo, para cualquier n, la proposición:

$Q(n) =$ "$P(n)$ y $P(n+1)$ y $P(n+2)$"

Obsérvese que $Q(n)$ es equivalente a:

"Cada uno de los tres enteros n, $n+1$ y $n+2$ es suma de 3 y de 8."

Demostramos el caso base $Q(14)$, que dice que cada uno de los tres enteros 14, 15 y 16 es suma de 3 y de 8. Lo hacemos exhibiendo descomposiciones explícitas:

$$\begin{aligned} 14 &= 8+3+3 \\ 15 &= 3+3+3+3+3 \\ 16 &= 8+8 \end{aligned}$$

Luego demostramos que, para cualquier $n \geq 14$, $Q(n)$ implica $Q(n + 1 =$. Para esto fijamos $n \geq 14$ y suponemos $Q(n)$ cierta. Tenemos que demostrar $Q(n+1)$, o sea: que $n+1$, $n+2$ y $n+3$ son sumas de 3 y 8. Cómo hemos supuesto $Q(n)$ cierta, tenemos que n, $n+1$ y $n+2$ son sumas de 3 y 8. Queda por demostrar que $n+3$ también. Cómo n es suma de 3 y 8, $n+3$ también (basta añadir una vez "3" a una descomposición de n). Por lo tanto, $Q(n+1)$ es cierta.

Hemos demostrado que $Q(n)$ implica $Q(n+1)$ y, justo antes, que $Q(14)$ es cierta. Por lo tanto $Q(n)$ es cierta para cualquier $n \geq 14$. Cómo consecuencia, todo entero $n \geq 14$ es suma de 3 y 8. $\diamondsuit$

.

3.5.2 *Inducción completa*

Existe una variación de la demostración por inducción, llamada *inducción completa*. Consiste en demostrar una sucesión de proposiciones $P(N)$, $P(N+1)$, $P(N+2)$ ...demostrando las dos proposiciones siguientes:

La inducción completa no es más que la inducción "simple", cambiando la hipótesis de recurrencia $P(n)$ por $Q(n) =$ "$P(N)$ y $P(N+1)$ y ... y $P(n)$".

1. la demostración de la primera proposición (caso base, $P(N)$) o de unas cuántas primeras (casos bases).
2. la demostración del hecho que cada proposición, excepto los casos bases, esta implicada por todas las anteriores. Es decir, para cualquier $n \geq N$

$$P(N) \text{ y } P(N+1) \text{ y } P(N+2) \text{ y } \cdots \text{ y } P(n-1) \text{ y } P(n) \Rightarrow P(n+1)$$

Ejemplo 3.5.4.
Vamos a demostrar formalmente que todo entero superior o igual a 2 es un producto de números primos (aceptamos lo productos de un solo factor). Recordamos que un número primo es un número positivo, distinto de 1, que no tiene más divisores (positivos) que él mismo y 1.

Para cualquier $n > 0$, sea $P(n)$ la proposición:

> El entero n es un producto de números primos.

Demostramos en primer lugar el caso base $P(2)$. Cómo 2 es primo, es un producto de primos.

Demostramos ahora que cada proposición $P(n)$, para $n > 2$, es implicada por la conjunción de $P(2)$ y $P(3)$ y ... y $P(n-1)$. Para esto, fijamos $n > 2$ y suponemos todas estas proposiciones $P(2), P(3), \ldots,$ $P(n-1)$ ciertas. Significa que cualquier entero k que cumple $2 \leq k \leq n-1$ es un producto de primos. Para el entero n hay dos casos:

- Caso n primo: en este caso, n es bien un producto de primos (un producto de un solo factor).
- Caso n no primo: observamos que n admite algún divisor k diferente de 1 y n (sino, ya que $n \neq 1$, n sería primo). Sea $j = n/k$. Tenemos también $1 < j < n$ (cómo consecuencia de $1 < k < n$). Por lo tanto $P(j)$ y $P(k)$ son ciertas: los enteros j y k son productos de primos. Cómo $n = j \cdot k$, es también un producto de primos.

En ambos casos, $P(n)$ es cierta.

Hemos demostrado que $P(2)$ es cierta y que para cada $n > 2$, $P(n)$ es implicada por $P(2)$ y $P(3)$ y ... y $P(n-1)$. Por inducción completa, concluimos que $P(n)$ es cierta para cualquier $n \geq 2$. $\diamondsuit$

4
Aritmética

4.1 Introducción: ecuaciones lineales diofánticas

Este tema presenta los objetos básicos del aritmética (divisores, números primos, máximo común divisor) y su estudio continuará en el tema siguiente (aritmética modular) dónde, además, podremos utilizar los conocimientos adquiridos para entender unas aplicaciones del aritmética (el sistema de criptografía RSA en particular).

Como motivación para este tema, consideramos el problema siguiente:

> Sean a, b y c enteros. Hallar todas las soluciones x, y *enteras* de la ecuación $ax + by = c$.

La ecuación $ax + by = c$ es una ecuación lineal, y ya sabemos encontrar todas sus soluciones reales: por ejemplo, si $b \leq 0$, es el conjunto de los puntos de la forma $(x, (c - ax)/b)$ para $x \in \mathbb{R}$. Decimos que $(x, (c - ax)/b)$ es la *solución general* de la ecuación, es decir una formula involucrando parámetros (aquí un único parámetro x) que describe todas las soluciones.

El problema que consideramos aquí es diferente, y de hecho, más complicado, porque buscamos solamente las soluciones con x e y enteros. Llamamos *ecuación diófantica* el problema de buscar solamente las soluciones enteras de una ecuación. Nuestro problema, por lo tanto, es resolver la ecuación diofántica $ax + by = c$ de incógnitas x e y.

La aritmética fue estudiada extensivamente por los griegos antiguos, y muchos objetos que presentaremos a continuación llevan nombre des matemáticos griegos de la antigüedad: las *ecuaciones diofánticas* fueron estudiadas por Diofanto de Alejandría, la *división euclídea* y el *algoritmo de Euclides* fueron descritos por Euclides, la *criba de Eratóstenes* por Eratóstenes. Se puede saber más sobre estos precursores en `http://gap-system.org/~history/BiogIndex.html`

Como siempre cuando se trata de ecuaciones, hay tres preguntas fundamentales:

- ¿ Admite soluciones ?
- ¿ Cuál es la forma del conjunto de las soluciones ?
- Dar una formula general para las soluciones (a lo mejor con parámetros). Esta formula general la llamaremos *solución general de la ecuación*.

Ejemplo 4.1.1.
Veamos en unos ejemplos la variedad de respuestas posibles a estas preguntas.

- La ecuación diofántica $x + y = 1$ tiene una infinidad de soluciones, son todos los pares de la forma $(1 - y, y)$ para $y \in \mathbb{Z}$.
- La ecuación diofántica $3x + 4y = 6$ tiene una infinidad de soluciones enteras: son todos los pares de la forma $(4k - 6, 6 - 3k)$ para k en $\mathbb{Z}$ (para esta ecuación, esto se puede demostrar, sin saber nada de la teoría que desarrollaremos, haciendo un simple cambio de variable $x' = x + y$ e $y' = y$). La expresión $(4k - 6, 6 - 3k)$ es la solución general de la ecuación.
- La ecuación diofántica $2x + 4y = 3$ no tiene ninguna solución entera. Es porque si x e y son enteros, entonces $2x + 4y$ debe ser par, y por lo tanto no puede ser igual a 3. Más generalmente, vemos que para que $ax + by = c$ admita soluciones, es necesario que cualquier divisor común de a y b divida también c.

Llegados a este punto, tenemos que reconocer que la situación es más complicada que para las ecuaciones lineales no diofánticas. ◊

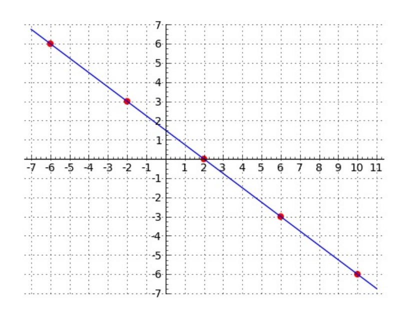


Figura 4.1: La ecuación $3x + 4y = 6$ tiene una infinidad de soluciones enteras. Son los puntos de la forma $(-6, 6) + k \cdot (4, -3)$ para $k \in \mathbb{Z}$.

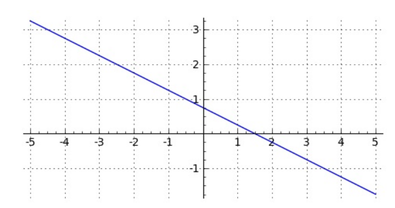


Figura 4.2: La ecuación $2x + 4y = 3$ no tiene ninguna solución entera. Dicho de otra manera: la recta de ecuación $2x + 4y = 3$ no pasa por ningún punto a coordenadas enteras.

En la resolución de las ecuaciones diofánticas $ax + by = c$, el *máximo común divisor* de a y b tiene un papel central. Antes de presentar un método de resolución de las ecuaciones diofánticas $ax + by = c$, introduciremos las nociones de aritmética que nos permitan entender y calcular este máximo común divisor.

4.2 *Aritmética con primos*

4.2.1 *Definiciones*

Empezamos con las definiciones de los objetos que nos interesarán en este parte del curso.

Definicion 4.2.1. *Sean a y b dos enteros. Se dice que a* divide *b cuando existe un entero k tal que $b = k\,a$. En este caso, se dice también que b* es un múltiplo de *a.*

Ejemplo 4.2.1.
Los múltiplos de 2 son los números pares. El número 0 tiene un solo múltiplo (él mismo) y todos los enteros son múltiplos de 1. ◊

Definicion 4.2.2. *Si a es un entero, entonces cuando hablamos de sus* divisores *nos referimos (en general, y siempre en estos apuntes) a sus divisores positivos, es decir todos los enteros positivos d que dividen a.*

Ejemplo 4.2.2.
Cualquier entero $n > 1$ tiene por lo menos dos divisores: él mismo y 1. Ciertos enteros no tienen más divisores, como 2, 3, 5, 7, 11 ... y otros tienen mucho más, cómo 12 (4 divisores además de 12 y 1) o 30 (6 divisores además de 1 y 30). ◊

En inglés: Mcd=gcd (greatest common divisor) y mcm=lcm (lowest common multiple).

Definicion 4.2.3. *Dados dos o más enteros, sus* divisores comunes *son los enteros positivos que les dividen todos, y su* máximo común divisor *(abreviación:* Mcd*) es el máximo de ellos. Sus* múltiplos comunes *son los enteros positivos que son múltiplos de todos, y su* mínimo común múltiplo *(abreviación:* mcm*) es el menor de ellos.*

Ejemplo 4.2.3.
Los enteros 9 y 4 tienen solamente un divisor común (el número 1). Es, por lo tanto, su Mcd. Al contrario, los números 24 y 36 tienen como divisores comunes: 1, 2, 3, 4, 6 y 12. Su Mcd es, por lo tanto, 12. ♢

Ejemplo 4.2.4.
Los enteros 9 y 4 no tienen ningún múltiplo común inferior a 36. Por lo tanto, 36 es su mcm. Al contrario, los números 24 y 36 admiten 72 como múltiplo común. Como no tienen ningún múltiplo común más pequeño, 72 es su mcm. ♢

Ejemplo 4.2.5.
Los números 6, 10 y 15 tienen un único divisor común (es 1). Es, por lo tanto, su Mcd. Su mcm es 30. ♢

Definicion 4.2.4. *Un entero $n > 1$ es* primo *si sus únicos divisores son* 1 *y n , y* compuesto *en el caso contrario.*

Por lo tanto, según esta definición, el número 1 no es ni primo ni compuesto.

Si, así es con la definición moderna de “entero primo”.

Damos ahora un procedimiento, llamado *Criba de Eratóstenes*, para obtener la lista de los primeros números primos. Digamos por ejemplo que queremos obtener la lista de los números primos no mayores que n, donde n es un entero.

1. Escribimos la lista de los enteros del 2 al n.
2. Mientras se quedan enteros no tachados:
   - Marcamos el primer entero no tachado.
   - Lo tachamos en la lista, y tachamos también todos sus múltiplos.

Entonces los primos inferiores o iguales a n son exactamente los números marcados.

Ejemplo 4.2.6.
Vamos a obtener todos los primos no mayores que 30 por medio del criba de Eratóstenes. Empezamos haciendo la lista de los números del 2 al 30.

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Marcamos el primer número de la lista (es 2) y lo tachamos, él y sus múltiplos (son todos lo números pares).

	[~~2~~]	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15
~~16~~	17	~~18~~	19	~~20~~	21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~

Marcamos el primer elemento no tachado que queda (el 3), y lo tachamos, él y sus múltiplos.

	[~~2~~]	[~~3~~]	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~
~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~

Marcamos el primer elemento no tachado que queda (el 5), y lo tachamos, él y sus múltiplos.

	[~~2~~]	[~~3~~]	~~4~~	[~~5~~]	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~
~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~

Y seguimos . . . Obtenemos al final (cuando todos los elementos están tachados):

	[~~2~~]	[~~3~~]	~~4~~	[~~5~~]	~~6~~	[~~7~~]	~~8~~	~~9~~	~~10~~	[~~11~~]	~~12~~	[~~13~~]	~~14~~	~~15~~
~~16~~	[~~17~~]	~~18~~	[~~19~~]	~~20~~	~~21~~	~~22~~	[~~23~~]	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	[~~29~~]	~~30~~

Hacemos ahora la lista de todos los elementos marcados:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29$$

Son todos los primos p que cumplen $p \leq 30$. ♢

Más tarde *demostraremos* el resultado siguiente, que aceptamos de momento:

Teorema 4.2.5 (Teorema de Euclides)**.** *Hay una infinidad de números primos.*

4.2.2 *El teorema fundamental del aritmética y sus consecuencias*

Teorema 4.2.6 (Teorema fundamental del aritmética, factorización única)**.** *Sea n un entero positivo. Entonces admite una descomposición cómo producto de potencias de primos distintos. Además, esta descomposición es única, excepto por el orden de los factores.*

Si notamos esta descomposición:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

con e_1, e_2, . . . e_k estrictamente positivos, entonces los números p_1, p_2, . . . , p_k son exactamente los divisores primos de n. Y para cada i, $p_i^{e_i}$ es la mayor potencia de p_i que divida n.

Ejemplo 4.2.7.
La descomposición de 12 es $12 = 2^2 \times 3^1$. En el teorema corresponde a $p_1 = 2$, $e_1 = 2$, $p_2 = 3$, $e_2 = 1$. Podemos escribir también esta descomposición cómo $12 = 3^1 \times 2^2$, correspondiendo a $p_1 = 3$, $e_1 = 1$, $p_2 = 2$, $e_2 = 2$ (es en este sentido que "la descomposición es única *excepto por el orden de los factores*"). ♢

Definicion 4.2.7. *Sea n un entero positivo y p un numero primo. Llamamos* multiplicidad de p en n *el mayor entero k tal que p^k divida n. Lo notamos $\mu_p(n)$.*

Ejemplo 4.2.8.
La descomposición en primos de 12 es $2^2 \times 3$. Según el teorema 4.2.6, los exponentes de 2 y 3 en esta descomposición son las multiplicidades de 2 y 3 en 12, es decir: $\mu_2(12) = 2$ y $\mu_3(12) = 1$. Según el teorema una vez m, los otros primos no dividen 12. por lo tanto, para cualquier primo p distinto de 2 y de 3 tenemos $\mu_p(12) = 0$. ♢

La descomposición en primos es bien útil para resolver los problemas sobre divisores y múltiplos de enteros. En efecto, tenemos las propiedades siguientes, que enunciamos sin demostración (hacer las demostraciones es un buen ejercicio):

- a divide b si y solo si para cualquier primo p, $\mu_p(a) \leq \mu_p(b)$.
- los divisores comunes de a_1, a_2, ..., a_k son los números n tal que para cualquier primo p, se tiene

$$\mu_p(n) \leq \text{mín}(\mu_p(a_1), \mu_p(a_2), \ldots, \mu_p(a_k)).$$

- los múltiplos comunes de a_1, a_2, ..., a_k son los números n tal que para cualquier primo p, se tiene

$$\mu_p(n) \geq \text{máx}(\mu_p(a_1), \mu_p(a_2), \ldots, \mu_p(a_k))$$

- En particular, si $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ y $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ con los p_i primos distintos, entonces el Mcd de a y b es:

$$p_1^{\text{mín}(e_1,f_1)} p_2^{\text{mín}(e_2,f_2)} \cdots p_k^{\text{mín}(e_k,f_k)}$$

y su mcm es:

$$p_1^{\text{máx}(e_1,f_1)} p_2^{\text{máx}(e_2,f_2)} \cdots p_k^{\text{máx}(e_k,f_k)}$$

- Como consecuencia importante del apartado anterior, y de la identidad: $\text{mín}(e, f) + \text{máx}(e, f) = e + f$, tenemos

$$Mcd(a, b) \times mcm(a, b) = a \times b.$$

- Otra consecuencia es: los divisores comunes de a y b son exactamente los divisores de su Mcd.
- Los múltiplos comunes de a y de b son exactamente los múltiplos de su mcm.

Se tiene $\text{mín}(e, f) + \text{máx}(e, f) = e + f$ porque de los dos enteros e y f, uno es el mín y el otro es el máx. Por lo tanto, $\text{mín}(e, f) + \text{máx}(e, f)$ es la suma de los dos números e y f.

Ejemplo 4.2.9.
Consideramos el entero $2^3 \times 3^5 \times 5^2 \times 11^7$. Sus divisores son exactamente los números de la forma $2^a 3^b 5^c 11^d$ con $0 \leq a \leq 3$ y $0 \leq b \leq 5$ y $0 \leq c \leq 2$ y $0 \leq d \leq 11$. Si queremos contarlos: tenemos 4 posibilidades para a (los valores 0, 1, 2 y 3), y 6 posibilidades para b, 3 posibilidades para c, y 8 posibilidades para d. En total, son $4 \times 6 \times 3 \times 8 = 576$ divisores. ♢

Ejemplo 4.2.10.
Si $a = 2^3 \times 3^5 \times 5 \times 7^2 \times 13^3$ y $b = 3 \times 5^2 \times 7^4 \times 11^3$ entonces $\mathrm{Mcd}(a, b) = 3 \times 5 \times 7^2$ y $\mathrm{mcm}(a, b) = 2^3 \times 3^5 \times 5^2 \times 7^4 \times 11^3 \times 13^3$. ♢

Ejemplo 4.2.11.
El Mcd de 24 y 36 es 12. Por lo tanto, su mcm es $(24 \times 36)/12 = 72$. ♢

Aquí viene una observación importante: por lo expuesto más arriba, calcular el Mcd de dos enteros (al igual que muchos otros problemas de aritmética) es extremadamente fácil cuando conocemos la descomposición en primos de por lo menos uno de los dos enteros. El problema es que *no conocemos ningún algoritmo computacionalmente eficiente para calcular la descomposición en primos de un entero*. En muchas aplicaciones del aritmética (por ejemplo en la criptografía RSA) con grandes enteros, no podemos contar sobre esta descomposición. Más abajo presentaremos un algoritmo muy eficiente (el algoritmo de Euclides) para calcular el Mcd (y resolver mucho más problemas) que no involucra la descomposición en primos.

Ejemplo 4.2.12.
Queremos calcular el Mcd de a y b con:

$$a = 12301866845301177551304949583849627207728535695\\
95334792197322452151726400507263657518745202199\\
78646938995647494277406384592519255732630345373\\
15482685079170261221429134616704292143116022212\\
40479274737794080665351419597459856902143413$$

y

$$b = 11207812846804988555387474152334412866415217\\
55728321836318470924068443481363048040124562O4\\
61213625439344884206057833500365635866467809 62\\
37746682834328013173162283008763927436881548 57\\
07422569774006565091930648179754454977613704261121$$

¡ Pero la descomposición en primos de a y b es muy difícil de obtener !
La descomposición de a por ejemplo es:

$$a =\\
33478071698956898786044169848212690817704794983\\
71376856891243138898288379387800228761471165 25\\
3174308773781446799948 9\\
\times\\
36746043666799590428244633799627952632279158164\\
34308764267603228381573966651127923337341714 33\\
968102700927987363089 17$$

Es el "récord del mundo" de factorización (en 2009), y necesitó 2 años de cálculos involucrando centenas de ordenadores ¡ En comparación, mi pequeño portátil encuentra (con SAGE) el Mcd de a y de b en menos de un milisegundo de tiempo CPU. No utiliza al descomposición en primos. Utiliza un algoritmo muy simple y muy eficiente que presentaremos en la sección siguiente, *el algoritmo de Euclides*.

¡ Inténtalo en el tuyo ! La instrucción para calcular el Mcd de a y b es `gcd(a,b)`.

$$\mathrm{Mcd}(a, b) =\\
33478071698956898786044169848212690817704794 98\\
37137685689124313889828837938780022876147116 5\\
2531743087737814467999489$$

◊

4.2.3 Demostraciones

A continuación vamos a *demostrar formalmente* dos resultados ya enunciados:

- El conjunto de los números primos es infinito (*Teorema de Euclides*).
- Cualquier entero positivo se descompone de manera única como producto de potencias de primos (*Teorema fundamental del aritmética*).

En las demostraciones nos basaremos solamente sobre los tres resultados siguientes:

- Cualquier conjunto no vacío de enteros positivos tiene un menor elemento. Es una propiedad fundamental de los números enteros que no se demuestra.
- Cualquier entero estrictamente superior a 1 es producto de primos. Esto ya fue demostrado en la parte sobre inducción matemática.
- Si un primo divide un producto de enteros, entonces necesariamente divide un factor del producto. O sea, si p es primo y divide $a_1 a_2 \cdots a_k$ entonces necesariamente p divide por lo menos uno de los enteros a_1, a_2, $\ldots$, a_k. Esto lo demostraremos más tarde, cuando tendremos las herramientas necesarias para hacerlo (el algoritmo de Euclides extendido y la noción de números *coprimos*).

Damos dos demostraciones del teorema de Euclides (El conjunto de los números primos es infinito).

Demostración 1 del Teorema de Euclides. Construimos por inducción una sucesión infinita de números primos p_1, p_2, p_3 distintos, ... Esto demostrará que hay una infinidad de primos.

Empezamos definiendo $p_1 = 2$. Luego, suponemos que ya hemos definido $p_1, p_2, \ldots, p_k$. Vamos a definir p_{k+1}. Para esto, consideramos el número $1 + p_1 p_2 \cdots p_k$. Es producto de primos, y, como es estrictamente superior a 1, admite en particular por lo menos un divisor primo. Definimos p_{k+1} cómo el menor divisor primo de $1 + p_1 p_2 \cdots p_k$. Nos queda a demostrar que es un "nuevo" primo, es decir que es distinto de $p_1, p_2, \ldots, p_k$. Si no fuese el caso, tendríamos que p_{k+1} divide el producto $p_1 p_2 \cdots p_k$. Cómo p_{k+1} divide también $1 + p_1 p_2 \cdots p_k$, deduciríamos que p_{k+1} divide 1. Es imposible porque 1 no tiene ningún divisor primo. Esto demuestra que p_{k+1} es distinto de los primos construidos anteriormente y acaba la demostración del teorema. □

k	$1 + p_1 p_2 \cdots p_k$	p_{k+1}
1	3	3
2	7	7
3	43	43
4	1807	13
5	23479	53
6	1244335	5
7	6221671	6221671
8	38709183810571	38709183810571

Cuadro 4.1: Los primeros números primos producidos por el algoritmo descrito en la primera demostración del teorema de Euclides.

La segunda demostración es una demostración por *reducción al absurdo*. Demostrar una proposición P por reducción al absurdo consiste en establecer que la negación P implica algo falso: $\neg P \Rightarrow f$.

Examinando la tabla de verdad de la implicación, vemos que en consecuencia P ha de ser falso.

Demostración 2 del teorema de Euclides. Suponemos que hay solamente un número finito de primos. Sea q su producto. Consideramos el número $1+q$. Como $1+q>1$ y como cada número superior a 1 es producto de primos, $1+q$ admite algún divisor primo p. Entonces p divide a la vez q y $1+q$. Por lo tanto p divide 1, ya que $1=(1+q)-q$. Es imposible, ya que 1 no tiene ningún divisor primo. Por contradicción, tenemos que concluir que la hipótesis según la cuál hay solamente un número finito de primos es falsa. Es decir, hay un número infinito de primos. □

Demostramos ahora el teorema fundamental del aritmética (Cualquier entero positivo se descompone de manera única como producto de potencias de primos).

Demostración del teorema fundamental del aritmética. Sea n un entero positivo. Ya hemos demostrado (en la parte "inducción") que si $n>1$, entonces n es primo o producto de primos. Abusando del lenguaje (pero sin dañar la coherencia matemática) nos permitiremos decir que si n es primo, también es producto de primos (es producto de un solo primo) y si $n=1$, también es producto de primos (es producto de 0 primos). Por lo tanto, n es producto de primos. Reagrupando los primos iguales en este producto obtenemos que n es producto de potencias de primos distintos,

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}.$$

Para demostrar la unicidad de la descomposición, vamos a proceder de la manera siguiente: demostraremos que para cualquiera descomposición de n de la forma

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$

con $p_1,p_2,\ldots,p_k$ distintos, se tiene que $e_1=\mu_{p_1}(n)$, $e_2=\mu_{p_2}(n)$, $\ldots$, $e_k=\mu_{p_k}(n)$. Esto establecerá que no hay otra descomposición que el producto de los $p^{\mu_p(n)}$ para los factores primos p de n.

Suponemos, por lo tanto, que

$$n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$$

con los primos p_i distintos y $k>0$ (si $k=0$ se tiene $n=1$, que tiene como única descomposición el "producto vacío", es decir, el producto con 0 factores).

Vamos a demostrar que $e_1=\mu_{p_1}(n)$, la multiplicidad de p_1 en n. Esto significa que tenemos que demostrar, por una parte, que $p_1^{e_1}$ divide n y, por otra parte, que si $f>e_1$ entonces p_1^f no divide n. Que $p_1^{e_1}$ divide n es evidente, ya que n es producto de $p_1^{e_1}$ y de otros números. Sea $f>e_1$. Demostremos que p_1^f no divide n. Observamos que la proposición

P="p_1^f divide n"

es equivalente a

Q="$p_1^{f-e_1}$ divide $p_2^{e_2} \cdots p_k^{e_k}$."

que implica

R="p_1 divide $p_2^{e_2} \cdots p_k^{e_k}$."

ya que $f - e_1 > 0$. Pero R es falsa. En efecto, como p_1 es distinto de $p_2, \ldots, p_k$ y que estos números son primos, p_1 no divide ninguno de ellos. Como p_1 es primo, no puede dividir un producto con factores $p_2, \ldots, p_k$.

En resumen, P es equivalente a Q que implica R, pero R es falsa. Por lo tanto, Q es falsa. En consecuencia, P es falsa también. Esto acaba la demostración de $e_1 = \mu_1(n)$.

Ahora sea $i \in \{2, \ldots, k\}$. La demostración de "$e_i = \mu_{p_i}(n)$" es la misma que la de "$e_1 = \mu_{p_1}(n)$" *mutatis mutandis*. En conclusión, $e_i = \mu_{p_i}(n)$ para cualquier i. □

4.3 *El algoritmo de Euclides*

4.3.1 *La división euclídea*

La "división euclídea" es simplemente la división con restos. Su buena definición esta garantizada por el teorema siguiente.

Teorema 4.3.1. *Sean a y b dos enteros con $b \neq 0$. Existe un único par (q, r) de enteros que cumpla las dos condiciones siguientes:*

1. $a = b\,q + r$.

2. $0 \leq r < |b|$.

Los enteros q y r se llaman cociente *y* resto *en la división euclídea de a entre b.*

Ejemplo 4.3.1.
La división de 152 por 50 es: $152 = 3 \times 50 + 2$. El cociente es 3, el resto es 2. ♢

Ejemplo 4.3.2.
Un número es impar si y solo si su resto en la división por 2 es 1. ♢

Ejemplo 4.3.3.
Tenemos $-13 = -3 \times 4 - 1$, pero esto no es la división de -13 entre 4, porque el resto no puede ser -1 (no puede ser negativo). La división de -13 entre 4 es $-13 = -4 \times 4 + 3$. ♢

Ejemplo 4.3.4.
La parte entera de un número real x es el único entero n (notado a menudo $[x]$) que cumple:

$$n \leq x < n + 1$$

Si x es el cociente a/b de dos enteros con $b > 0$, entonces estas desigualdades son equivalentes a:

$$bn \leq a < bn + b$$

Es equivalente a:

$$0 \leq a - bn < b$$

Reconocemos que $a - bn$ es el resto de la división de a entre b, y n es su cociente. En resumen, si $b > 0$, entonces $\left[\frac{a}{b}\right]$ es el cociente en la división euclídea de a entre b. ♢

Demostración del Teorema 4.3.1. Sea A el conjunto de los números de la forma $a - kb$ para $k \in \mathbb{Z}$. Entonces $A \cap \mathbb{N}$ es un subconjunto no vacío de $\mathbb{N}$. Por lo tanto admite un menor elemento r. Como r pertenece a A, existe un entero q tal que $a - qb = r$, es decir $a = qb + r$. Como r pertenece a $\mathbb{N}$, tenemos $r \geq 0$. Finalmente r no puede ser mayor o igual a $|b|$, sino $r - |b|$ sería otro elemento de $A \cap \mathbb{N}$, menor que r. Por lo tanto, $r < |b|$. Esto demuestra que existe por lo menos un par (q, r) que satisface las condiciones del teorema.

No podemos tener otro par (q', r') que cumpla las condiciones del teorema. En efecto, el intervalo $\{0, 1, \ldots, |b| - 1\}$ no puede contener dos números de la forma $a - kb$, ya que dos números tienen diferencia por lo menos b. Como ya contiene r, no puede contener otro $r' = a - q'b$. □

Tenemos la propiedad importante siguiente de la división euclídea.

Lema 4.3.2. *Sean a y b dos enteros, con $b \neq 0$. Sea r el resto en la división euclídea de a entre b. Entonces a y b por una parte, y b y r por otra parte, tienen exactamente los mismos divisores comunes. En particular, tienen el mismo* Mcd*:*

$$\text{Mcd}(a, b) = \text{Mcd}(b, r)$$

Ejemplo 4.3.5.
Digamos que queremos calcular el Mcd de 1483 y 517. Tenemos: $1483 = 2 \times 517 + 449$. Por lo tanto, el resto en la división euclídea de 1483 entre 517 es 449. Por lo tanto: $\text{Mcd}(1483, 517) = \text{Mcd}(517, 449)$. Hemos reducido el problema de calcular el Mcd de dos números en el problema de calcular el Mcd de números más pequeños. A continuación explotaremos esta idea más a fondo. ♢

4.3.2 *El algoritmo de Euclides (para calcular el* Mcd*)*

Ejemplo 4.3.6.
Continuamos con el ejemplo 4.3.5, donde queríamos calcular $\text{Mcd}(1483, 517)$. Lo hacemos utilizando varias veces el lema 4.3.2, reduciendo cada vez los enteros implicados por medio de una división euclídea.

$1483 = 2 \times 517 + 449,$	por lo tanto $\text{Mcd}(1483, 517) = \text{Mcd}(517, 449)$
$517 = 1 \times 449 + 68,$	por lo tanto $\text{Mcd}(517, 449) = \text{Mcd}(449, 68)$
$449 = 6 \times 68 + 41,$	por lo tanto $\text{Mcd}(449, 68) = \text{Mcd}(68, 41)$
$68 = 1 \times 41 + 27,$	por lo tanto $\text{Mcd}(68, 41) = \text{Mcd}(41, 27)$
$41 = 1 \times 27 + 14,$	por lo tanto $\text{Mcd}(41, 27) = \text{Mcd}(27, 14)$
$27 = 1 \times 14 + 13,$	por lo tanto $\text{Mcd}(27, 14) = \text{Mcd}(14, 13)$
$14 = 1 \times 13 + 1,$	por lo tanto $\text{Mcd}(14, 13) = \text{Mcd}(13, 1)$
$13 = 13 \times 1 + 0,$	por lo tanto $\text{Mcd}(13, 1) = \text{Mcd}(1, 0).$

Al llegar aquí concluimos que $\text{Mcd}(1483, 517) = \text{Mcd}(1, 0)$. Observamos que los divisores de 0 son todos los enteros. Por lo tanto los divisores comunes de 0 y de 1 son simplemente los divisores de 1. Hay solamente 1. Por lo tanto, el Mcd de 0 y 1 es 1. ◊

Este procedimiento para calcular el Mcd de dos enteros funciona siempre y, además es computacionalmente eficaz. Se llama el *algoritmo de Euclides*. En dos palabras, el algoritmo de Euclides define una "sucesión de restos", cuyos dos primeros términos son a y b, tal que cada nuevo término es el resto en la división de los dos anteriores. Aquí esta una definición más formal:

> Definimos recursivamente una sucesión $(r_1, r_2, r_3, \ldots)$ por medio de
>
> - las condiciones iniciales: $r_1 = a$, $r_2 = b$,
> - y de la relación: para cualquier $i \geq 2$, si r_{i-1} y r_{i-2} son definidos y $r_{i-1} \neq 0$, entonces r_i es el resto en la división de r_{i-2} entre r_{i-1}.
>
> La sucesión así producida es finita, y el Mcd de a y b es el ultimo término diferente de 0.

La sucesión así definida es finita porque a cualquier etapa, se tiene, por definición de la división euclídea, para cualquier $i \geq 2$, $0 \leq r_i < r_{i-1}$.

Ejemplo 4.3.7. (Continuación del ejemplo ??).
La sucesión de los restos en el algoritmo de Euclides aplicado a 1483 y 517 es:

$$517, 449, 69, 41, 28, 13, 2, 1, 0$$

El Mcd es 1 y se obtiene como ultimo resto distinto de 0. ◊

4.3.3 El algoritmo de Euclides extendido

Empezamos con una definición.

Definicion 4.3.3. *Si a y b son dos enteros, las* combinaciones lineales a coeficientes enteros de *a y b son las expresiones de la forma $ax + by$ con x e y enteros.*

Obsérvese que si a y b son enteros y si $a = bq + r$ es la división euclídea de a entre b, entonces r es una combinación lineal de a y de

b. En efecto, $r = a - q\,b$ Podemos utilizar esta descomposición del resto en cada etapa del algoritmo de Euclides.

$r = a - qb$, es bien una combinación lineal de a y de b, los coeficientes son $x = 1$ e $y = -q$.

Ejemplo 4.3.8.
Aplicamos el algoritmo de Euclides a $a = 1483$ y $b = 517$. En cada paso:

1. Dividimos el penúltimo resto obtenido por el ultimo resto obtenido, esto produce un nuevo resto (es el algoritmo de Euclides "no extendido").
2. Aislamos el nuevo resto para expresarlo como combinación lineal de los dos restos anteriores.
3. Sustituimos en esta combinación lineal las expresiones de estos dos restos anteriores en función de a y b.
4. Simplificamos: obtenemos una descomposición del nuevo resto como combinación lineal de a y b.

Estos cuatro etapas corresponden a las cuatro columnas de la tabla siguiente:

División	Aislar el nuevo resto	Sustituir	Simplificar
$1483 = 2 \times 517 + 449$	$449 = 1483 - 2 \times 517$	$= a - 2\,b$	
$517 = 1 \times 449 + 68$	$68 = 517 - 449$	$= b - (a - 2b)$	$= -a + 3b$
$449 = 6 \times 68 + 41$	$41 = 449 - 6 \times 68$	$= (a - 2b) - 6(3b - a)$	$= 7a - 20b$
$68 = 1 \times 41 + 27$	$27 = 68 - 41$	$= (3b - a) - (7a - 20b)$	$= -8a + 23b$
$41 = 1 \times 27 + 14$	$14 = 41 - 27$	$= (7a - 20b) - (-8a + 23b)$	$= 15a - 43b$
$27 = 1 \times 14 + 13$	$13 = 27 - 14$	$= (-8a + 23b) - (15a - 43b)$	$= -23a + 66b$
$14 = 1 \times 13 + 1$	$1 = 14 - 13$	$= (15a - 43b) - (-23a + 66b)$	$= 38a - 109b$
$13 = 13 \times 1 + 0$			

En conclusión, el Mcd de 1483 y 517 es 1 y tenemos la descomposición: $1 = 38 \times 1483 - 109 \times 517$. ◊

El "algoritmo de Euclides extendido" consiste en aplicar el algoritmo de Euclides y, además, a cada paso, descomponer el nuevo resto r_i como combinación lineal de a y b, utilizando para esto las descomposiciones de los dos restos anteriores r_{i-1} y r_{i-2} como combinaciones lineales de a y b. Produce, al final, una descomposición lineal del Mcd de a y b como combinación lineal de a y b.

Sacamos ahora unas consecuencias teóricas de la existencia del algoritmo de Euclides.

Lema 4.3.4. *Sean a y b dos enteros con $b \neq 0$. Entonces $\operatorname{Mcd}(a,b)$ es una combinación lineal de a y b. Y, en consecuencia, cualquier múltiplo de a y b es también combinación lineal de a y b.*

Demostración. El algoritmo de Euclides extendido proporciona una descomposición de $\operatorname{Mcd}(a,b)$ como combinación lineal de a y b, es decir una descomposición de la forma:

$$\operatorname{Mcd}(a,b) = xa + yb$$

Ahora, sea m un múltiplo de $\text{Mcd}(a,b)$. Existe un entero k tal que $m = k\,\text{Mcd}(a,b)$. Por lo tanto,

$$m = k(xa + yb) = kxa + kyb$$

Vemos que m es combinación lineal de a y b (con coeficientes kx y ky). □

Definicion 4.3.5. *Sean a y b dos enteros. Una* identidad de Bézout *para a y b es una descomposición de* $\text{Mcd}(a,b)$ *como combinación lineal de a y b, es decir una expresión de la forma:*

$$\text{Mcd}(a,b) = xa + yb$$

Tenemos dos conjuntos: por una parte, el conjunto de los múltiplos de $\text{Mcd}(a,b)$, cuya estructura es clara, y por otra parte, el conjunto de las combinaciones lineales de a y b, que parece más enredado. Acabamos de establecer que el primero es estos conjuntos esta contenido en el otro. Ahora viene el resultado fuerte: ¡ los dos conjuntos son iguales !

Teorema 4.3.6. *Sean a y b dos enteros, con* $b \neq 0$*. Entonces las combinaciones lineales de a y b son exactamente los múltiplos de* $\text{Mcd}(a,b)$*.*

Demostración. Ya hemos demostrado que cualquier múltiplo de $\text{Mcd}(a,b)$ es combinación lineal de a y b. Nos queda por demostrar que cualquiera combinación lineal de a y b es múltiplo de $\text{Mcd}(a,b)$. Es bastante elemental. Consideremos una combinación lineal de a y b, es decir un número de la forma $xa + yb$ con x e y enteros. Notemos d para $\text{Mcd}(a,b)$. Como d es un divisor común de a y b, existen enteros u y v tal que $a = ud$ y $b = vd$. Por lo tanto, $xa + yb = xud + yvd = (xu + yv)d$. Es un múltiplo de d. □

Más consecuencias, esta vez en relación con el problema de las ecuaciones diofánticas lineales.

Teorema 4.3.7. *Consideramos la ecuación diofántica lineal* $ax + by = c$ *con a, b, c enteros y* $b \neq 0$*. Admite soluciones si y solo si c es un múltiplo de* $\text{Mcd}(a,b)$*.*

Demostración. En efecto, las soluciones (x,y) de $ax + by = c$ son exactamente los coeficientes en las descomposiciones de c como combinación lineal de a y b. En particular, la ecuación admite soluciones si y solo si c admite descomposiciones como combinación lineal de a y b. Por el teorema anterior, es equivalente a: "c es un múltiplo de $\text{Mcd}(a,b)$". □

Ejemplo 4.3.9.
La ecuación $105x + 42y = 30$ no admite ninguna solución. En efecto, calculamos (con el algoritmo de Euclides) que $\text{Mcd}(105,42) = 21$ y 21 no divide 30. ◊

Ejemplo 4.3.10.
Sea c un entero. La ecuación $1483x + 517y = c$ admite siempre soluciones, independientemente del valor de c. En efecto, hemos calculado que $\text{Mcd}(1483, 517) = 1$, siempre divide c. ♢

4.3.4 *Números coprimos*

Definicion 4.3.8. *Sean a y b dos enteros. Decimos que a y b son* coprimos *(o que son* primos entre si*) cuando su único divisor común es* 1*, es decir, cuando su* Mcd *vale* 1*.*

Una manera corta de demostrar a alguien que dos números a y b son coprimos (sin enseñarle toda la ejecución del algoritmo de Euclides que calcula que $\text{Mcd}(a, b) = 1$) consiste en enseñarle una identidad de Bézout $ax + by = 1$.

Ejemplo 4.3.11.
Para certificar que 1487 y 512 son coprimos, basta enseñar la identidad de Bézout:

$$1 = 38 \times 1483 - 109 \times 517$$

♢

Ejemplo 4.3.12.
Dos enteros consecutivos n y $n + 1$ son siempre coprimos, ya que tenemos la identidad de Bézout:

$$1 = (-1) \times n + 1 \times (n + 1)$$

♢

Ejemplo 4.3.13.
Sean a, b y c enteros con $b \neq 0$. La ecuación $ax + by = c$ define una recta del plano, y $(-b, a)$ es un vector director de la recta. Sea d el Mcd de a y b y $\alpha = a/d$, $\beta = b/d$. Entonces $(-\beta, \alpha)$ es también un vector director de la recta. Los enteros α y β con coprimos. En efecto, como $d = \text{Mcd}(a, b)$, tenemos una identidad de Bézout $d = ua + vb$. Dividiendo ambos lados por d obtenemos $1 = u\alpha + v\beta$. Esta nueva identidad de Bézout certifica que α y β son coprimos.

Los vectores $(-\beta, \alpha)$ y $(\beta, -\alpha)$ son los únicos vectores directores de la recta de coordenadas enteras coprimas. Son también los más pequeños vectores directores de la recta de coordenadas enteras. ♢

Por ejemplo, para la recta de ecuación $81x + 153y = 36$, los más pequeños vectores directores de coordenadas enteras son $(-17, 9)$ y $(17, -9)$, ya que el Mcd de 81 y 153 es 9, y que $(-153, 81) = 9 \cdot (-17, 9)$.

Vemos que a y b son coprimos cuando 1 es combinación lineal de a y b, es decir, cuando existen enteros x e y tal que $1 = xa + yb$. Pero en este caso, cualquier entero k es también combinación lineal de a y b. En efecto, tenemos $k = (kx)a + (ky)b$. Esto caracteriza de manera alternativa los pares de números coprimos.

Proposición 4.3.9. *Sean a y b dos enteros. Entonces a y b son coprimos si y solo si todos los enteros pueden obtenerse como combinaciones lineales de a y b.*

Veamos a que corresponde la noción de "coprimos" cuando uno de los enteros es primo. Si a es un entero y p un primo, tenemos la alternativa siguiente:

- p divide a. Entonces $\text{Mcd}(a, p) = p$. En particular, a y p no son coprimos.
- p no divide a. Como los únicos divisores de p son p y 1, y que p no es divisor de a, vemos que el único divisor común de a y p es 1. Por lo tanto a y p son coprimos.

Por lo tanto, si p es primo, entonces a y p son coprimos si y solo si a no es múltiplo de p.

La proposición y el teorema siguientes son importantes. Bastan para justificar la introducción de la noción de "coprimos".

Proposición 4.3.10. *Sean a, b, n enteros. Si n divide ab y si, además, n y a son coprimos, entonces n divide b.*

Demostración. Suponemos que n divide ab y que n y a son coprimos. Como n divide ab, existe un entero k tal que $ab = kn$. Como n y a son coprimos, existen enteros x e y tal que $1 = xa + yn$ (identidad de Bézout). Por lo tanto, $xa = 1 - yn$. Multiplicamos la identidad $ab = kn$ por x. Esto da $xab = xkn$. Sustituimos xa por $1 - yn$, obtenemos $(1 - yn)b = xkn$. Desarrollamos y reagrupamos los términos involucrando n, obtenemos: $b = (yb + xk)n$. Vemos que n divide b. □

Teorema 4.3.11. *Sea p un número primo. Si p divide un producto $a_1a_2 \cdots a_k$, entonces necesariamente divide por lo menos uno de los factores a_1, a_2, ..., a_k.*

Demostración. Se demuestra por inducción sobre k. Nuestra hipótesis de inducción es:

> $P(k) =$"Si p divide un producto de k enteros entonces divide por lo menos uno de ellos."

Incluimos en esta sucesión de proposiciones el caso $k = 1$. Un producto de un solo entero a es simplemente este entero.

Nuestro caso base será $k = 1$. La proposición $P(1)$ dice que si p divide un entero a, entonces p divide por lo menos uno de los elementos de la lista (a) ¡ Es una lista de un solo elemento ! En fin, $P(1)$ dice que si p divide a, entonces p divide a. Por lo tanto $P(1)$ es cierta.

Demostramos ahora que cada una de las proposiciones $P(k)$ implica la siguiente, $P(k+1)$, para cualquier $k \geq 1$.

Sea $k \geq 1$. Suponemos $P(k)$ cierta. Sean a_1, a_2, ..., a_{k+1} enteros tal que p divide el producto $a_1a_2 \cdots a_{k+1}$. Hay dos casos:

- o bien p divide a_{k+1}.
- o bien p no divide a_{k+1}. En este caso p y a_{k+1} son coprimos. Utilizando la proposición 4.3.10 deducimos que p divide $a_1a_2 \cdots a_k$. Pero, como hemos supuesto $P(k)$ cierto, podemos deducir que p divide por lo menos uno de los enteros a_1, a_2, ..., a_k.

En ambos casos, p divide por lo menos uno de los factores del producto. Por lo tanto $P(k+1)$ es cierta.

Hemos demostrado que $P(k)$ implica $P(k+1)$ para cualquier $k \geq 1$. Esto establece (junto con la demostración de $P(1)$) por inducción que $P(k)$ es cierta para cualquier k. □

Recordamos que el teorema 4.3.11 fue utilizado para demostrar el teorema fundamental del aritmética (sobre la descomposición en primos) y el teorema de Euclides (sobre la infinidad de los números primos)

4.4 Resolución de la ecuación diofántica lineal $ax + by = c$

Vamos a presentar un método de resolución de la ecuación diofántica

$$ax + by = c$$

dónde a, b y c son enteros y $a \neq 0$ o $b \neq 0$.

Se puede resolver la ecuación diofántica $ax + by = c$ en cuatro etapas.

1. Determinar si la ecuación tiene soluciones, o no.
2. Hallar una solución particular de $ax + by = c$.
3. Hallar la solución general de la ecuación homogénea, $ax + by = 0$.
4. Hacer la suma de estas dos soluciones: es la solución general de $ax + by = c$.

Ya hemos observado que la ecuación admite soluciones si y solo si $\text{Mcd}(a, b)$ divide c, y como hallar una solución particular con el algoritmo de Euclides extendido. A continuación explicamos el tercer paso, y luego repasaremos las cuatro etapas en detalle.

4.4.1 La ecuación lineal homogénea asociada

La *ecuación lineal homogénea asociada* a $ax + by = c$ es la ecuación obtenida cancelando el término independiente c. Es:

$$ax + by = 0$$

Proposición 4.4.1. *Sean a, b y c enteros, con $a \neq 0$ o $b \neq 0$, tal que* $\text{Mcd}(a, b)$ *divide c. La solución general de la ecuación diofántica $ax + by = c$ es la suma de:*

- *la solución general de la ecuación lineal diofántica asociada, $ax + by = 0$,*
- *y de una solución cualquiera de $ax + by = c$.*

Demostración. Sea (x_0, y_0) una solución cualquiera de $ax + by = c$. Entonces: $ax + by = 0$ es equivalente a: $ax + by + ax_0 + by = c$ (ya que $ax_0 + by_0 = c$). Es equivalente a $a(x + x_0) + b(y + y_0) = c$, es decir a que $(x + x_0, y + y_0)$ sea solución de $ax + by = c$. Por lo tanto, (X, Y) es la solución general de $ax + by = c$ si y solo si $(X, Y) + (x_0, y_0)$ es la solución general de $ax + by = c$. □

Ejemplo 4.4.1.
La solución general de $3x + 4y = 6$ es $(4k - 6, 6 - 3k)$. Se descompone como $(4k, -3k) + (-6, 6)$. La expresión $(4k, -3k)$ es la solución general de $3x + 4y = 0$, y $(-6, 6)$ es una solución particular de $3x + 4y = 6$. $\Diamond$

Resolver una ecuación lineal diofántica homogénea $ax + by = 0$ es fácil. En primer lugar, simplificamos por el Mcd de a y b. A continuación (proposición 4.4.2) demostraremos que la nueva ecuación que obtenemos tiene sus coeficientes primos entre si. Y luego (proposición 4.4.3) veremos que es inmediato resolver una ecuación lineal dióфantica homogénea con coeficientes primos entre sí.

Proposición 4.4.2. *Sean a y b enteros, con $a \neq 0$ o $b \neq 0$. Sean α y β los enteros definidos por $\alpha = a / \operatorname{Mcd}(a, b)$ y $\beta = b / \operatorname{Mcd}(a, b)$. Entonces α y β son primos entre si.*

Demostración. Suponemos $b \neq 0$ (el caso $a \neq 0$ se trata de manera similar).

La ecuación $ax + by = 0$ es equivalente a $\alpha x + \beta y = 0$ (hemos dividido ambos lados de la ecuación por $\operatorname{Mcd}(a, b)$).

Afirmamos que α y β son coprimos. En efecto, existen enteros u y v tal que $\operatorname{Mcd}(a, b) = au + bv$ (identidad de Bézout; el Mcd es combinación lineal de a y b). Dividiendo ambos lados por $\operatorname{Mcd}(a, b)$ obtenemos $1 = \alpha u + \beta v$. Esta identidad de Bézout certifica que α y β son coprimos. $\square$

Proposición 4.4.3. *Sean α y β enteros, con $\alpha \neq 0$ o $\beta \neq 0$. Entonces la solución general de la ecuación lineal homogénea diofántica $\alpha x + \beta y = 0$ es $(-\beta k, \alpha k)$ con k parámetro.*

Demostración. Le ecuación $\alpha x + \beta y = 0$ es equivalente a $-\alpha x = \beta y$.

Sea (x, y) una solución. Vemos que β divide αx. Como β y α son coprimos, obtenemos que β divide $-x$ (hemos utilizado la proposición 4.3.10). Esto significa que existe un entero k tal que $x = -k\beta$. Como $x- = k\beta$ y $-\alpha x = \beta y$, obtenemos que $\alpha k \beta = \beta y$. Como $\beta \neq 0$, podemos simplificar por β. Obtenemos $y = \alpha k$. En resumen, si (x, y) es una solución, entonces existe un entero k tal que $x = -\beta k$ e $y = \alpha k$.

Recíprocamente, es inmediato comprobar, por cálculo directo, que para cualquier entero k, el par $(-\beta k, \alpha k)$ es solución de la ecuación $ax + by = 0$, ya que $a\beta = \operatorname{Mcd}(a, b)\alpha\beta$ y $b\alpha = \operatorname{Mcd}(a, b)\beta\alpha$.

Por lo tanto, hemos demostrado que la solución general de $ax + by = 0$ es $(\beta k, -\alpha k)$ con k parámetro. $\square$

4.4.2 *Resolución de la ecuación lineal diofántica $ax + by = c$*

Detallamos a continuación las cuatro etapas de la resolución evocadas anteriormente.

1. **Determinar si la ecuación tiene soluciones, o no.** Utilizamos el criterio del teorema 4.3.7: la ecuación admite soluciones si y solo si el Mcd de a y b divide c. Calculamos, por lo tanto, el Mcd de a

y b (con el algoritmo de Euclides). Si no hay solución el problema esta resuelto.

2. **Hallar una solución particular de $ax + by = c$.** Una tal solución particular es proporcionada por la identidad de Bézout. En efecto, la identidad de Bézout es de la forma $ua + vb = \text{Mcd}(a, b)$. En el etapa anterior hemos determinado que $\text{Mcd}(a, b)$ divide c. Encontramos el entero m tal que $c = m\,\text{Mcd}(a, b)$. Multiplicamos la identidad de Bézout por m, obtenemos: $(mu)a + (mv)b = m\,\text{Mcd}(a, b) = c$. Por lo tanto, $x = mu$ con $y = mv$ es una solución particular de la ecuación.

3. **Hallar la solución general de la ecuación homogénea, $ax + by = 0$.** Se hace por medio de la proposición 4.4.3.

4. **Hacer la suma de estas dos soluciones: es la solución general de $ax + by = c$.** Sin comentario.

Ejemplo 4.4.2.
Resolvamos la ecuación diofántica $227271x + 737814y = 53229$.

En primer lugar, aplicamos el algoritmo de Euclides a los coeficientes 737814 y 227271 para calcular su Mcd y determinar si la ecuación admite soluciones.

$$\begin{aligned}
737814 &= 3 \times 227271 + 56001 \\
227271 &= 4 \times 56001 + 3267 \\
56001 &= 17 \times 3267 + 462 \\
3267 &= 7 \times 462 + 33 \\
462 &= 14 \times 33 + 0
\end{aligned}$$

Vemos que el Mcd de 737814 y 227271 es 33. Comprobamos que 33 divide 53229. En efecto, $53229 = 33 \times 1613$. Por o tanto la ecuación admite soluciones enteras.

Luego, buscamos alguna solución de la ecuación. Para esto, ponemos $a = 227271$ y $b = 737814$ y expresamos el Mcd como combinación lineal de a y b, por medio del algoritmo de Euclides extendido. Nos dará una identidad de Bézout: $\text{Mcd}(a, b) = ua + vb$. Como $53229 = \text{Mcd}(a, b) \times 1613$, multiplicaremos por 1613 y obtendremos una descomposición: $53229 = (1613u)a + (1613v)b$, correspondiendo a una solución $x = 1613u$, $y = 1613v$.

No necesitamos repetir todos los cálculos, utilizamos las divisiones euclídeas realizadas en la etapa anterior.

$b = 3 \times a + 56001$	$56001 = -3a + b$		
$a = 4 \times 56001 + 3267$	$3267 = a - 4 \times 56001$	$= a - 4(-3a + b)$	$= 13a - 4b$
$56001 = 17 \times 3267 + 462$	$462 = 56001 - 17 \times 3267$	$= (-3a + b) - 17(13a - 4b)$	$= -224a + 69b$
$3267 = 7 \times 462 + 33$	$33 = 3267 - 7 \times 462$	$= (13a - 4b) - 7(-224a + 69b)$	$= 1581a - 487b$

Obtenemos la identidad de Bézout $33 = 1581a - 487b$. Multiplicamos ambos lados por 1613, obtenemos:

$$53\,229 = 2\,555\,153a - 785\,531b$$

Por lo tanto, una solución particular es $x = 2\,555\,153$, $y = -785\,531$.

Luego resolvemos la ecuación homogénea asociada. Es $227271x + 737814y = 0$. Dividiendo por el Mcd de los coeficientes obtenemos una ecuación equivalente con coeficientes coprimos:

$$6887x + 22358b = 0$$

Como los coeficientes son coprimos, la solución general es $(-22358k, 6887k)$.

En conclusión, la solución general de la ecuación diofántica $227271x + 737814y = 53229$ es $(2\,555\,153 - 22358k, 737814 + 6887k)$. ♢

Ejemplo 4.4.3.
Resolvamos la ecuación diofántica $143x + 231y = 321$.

Calculamos el Mcd de 143 y 231 por medio del algoritmo de Euclides.

Como 143 y 231 son pequeños, podríamos también calcular su Mcd descomponiéndolos en primos, sin aplicar el algoritmo de Euclides.

$$\begin{aligned} 231 &= 1 \times 143 + 88 \\ 143 &= 1 \times 88 + 55 \\ 88 &= 1 \times 55 + 33 \\ 55 &= 1 \times 33 + 22 \\ 33 &= 1 \times 22 + 11 \\ 22 &= 1 \times 11 + 0 \end{aligned}$$

El ultimo resto no nulo es 11, es el Mcd de 213 y 143. Dividiendo 321 entre 11 obtenemos: $321 = 29 \times 11 + 2$. Por lo tanto 11 no divide 321. Concluimos que la ecuación no tiene solución entera. ♢

Ejemplo 4.4.4.
A continuación, resolvemos el problema siguiente:

> Hemos gastado 85, 39 euros en bolígrafos y cuadernos. Cada bolígrafo costaba 1, 27 euros, y cada cuaderno costaba 3, 23 euros. ¿ Cuantos bolígrafos y cuántos cuadernos fueron comprados, al mínimo ?

Sea x el número de bolígrafos e y el numero de cuadernos. Expresamos los precios en céntimos. Tenemos la relación $127x + 323y = 8539$.

Comprobamos que la ecuación admite soluciones enteras calculando el Mcd de 127 y 323 con el algoritmo de Euclides.

$$\begin{aligned} 323 &= 2 \times 127 + 69 \\ 127 &= 1 \times 69 + 58 \\ 69 &= 1 \times 58 + 11 \\ 58 &= 5 \times 11 + 3 \\ 11 &= 3 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

El Mcd de 127 y 323 es 1. Por lo tanto la ecuación admite soluciones.

Buscamos ahora una solución de la ecuación por medio del algoritmo de Euclides extendido. Ponemos $a = 127$ y $b = 323$

$$\begin{array}{r|llll} b = 2 \times a + 69. & 69 & = b - 2a & & \\ a = 1 \times 69 + 58. & 58 & = a - 69 & = a - (b - 2a) & = 3a - b \\ 69 = 1 \times 58 + 11. & 11 & = 69 - 58 & = (b - 2a) - (3a - b) & = -5a + 2b \\ 58 = 5 \times 11 + 3. & 3 & = 58 - 5 \times 11 & = (3a - b) - 5(-5a + 2b) & = 28a - 11b \\ 11 = 3 \times 3 + 2. & 2 & = 11 - 3 \times 3 & = (-5a + 2b) - 3(28a - 11b) & = -89a + 35b \\ 3 = 1 \times 2 + 1. & 1 & = 3 - 2 & = (28a - 11b) - (-89a + 35b) & = 117a - 46b \end{array}$$

Por lo tanto, $117a - 46b = 1$. Multiplicando por 8539 obtenemos $999\,063a - 392\,794b = 8\,539$. Vemos que una solución particular de la ecuación es $(x, y) = (999\,063, -392\,794)$.

Resolvemos ahora la ecuación homogénea asociada. Es $127x + 323y = 0$. Como 127 y 323 son coprimos, su solución general es $(-323k, 127k)$. Finalmente, la solución general de la ecuación diofántica $127x + 323y = 8539$ es $(x, y) = (999\,063 - 323k, -392\,794 + 127k)$.

Añadimos ahora las condiciones $x \geq 0$ e $y \geq 0$, ya que las cantidades de bolígrafos y de cuadernos no pueden ser negativas. Para $(x, y) = (999\,063 - 323k, -392\,794 + 127k)$, son equivalentes a

$$999\,063 - 323k \geq 0, \qquad -392\,794 + 127k \geq 0$$

Son equivalentes a:

$$392\,794/127 \leq k \leq 999\,063/323$$

Realizando las divisiones euclídeas de 392 794 entre 127 y 999 063 entre 323 simplificamos las desigualdades en

$$3092 + 110/127 \leq k \leq 3093 + 24/323$$

Para k entero son equivalentes a:

$$3093 \leq k \leq 3093$$

Por lo tanto hay una única solución, corresponde a $k = 3093$. Calculamos que esta solución es $x = 24$ e $y = 17$. Hemos comprado 24 bolígrafos y 17 cuadernos. ♢

Ejemplo 4.4.5.
A veces, cuando la ecuación es especialmente sencilla, podemos utilizar atajos para resolverla, en vez de aplicar estrictamente el método propuesto en estos apuntes. Veamos como resolver la ecuación diofántica $81x + 153y = 36$.

Calculamos el Mcd de 81 y 153. Los números son suficientemente pequeños para hacerlo utilizando la descomposición en primos. Tenemos $81 = 3^4$. Calculamos que $153 = 3 \times 51 = 3 \times 3 \times 17$. Por lo tanto $\text{Mcd}(81, 153) = 3^2$. Divide 36. Por lo tanto, la ecuación admite soluciones enteras. Podemos simplificar la ecuación, dividendo todo por 9; la ecuación es equivalente a $9x + 17y = 4$. Los nuevos coeficientes 9 y 17 son coprimos.

En vez de calcular una identidad de Bézout para 9 y 17 por medio del algoritmo de Euclides, encontramos una identidad de Bézout "evidente": $2 \times 9 - 17 = 1$. Deducimos (multiplicando por 4) que $8 \times 9 - 4 \times 17 = 4$. Por lo tanto $(x, y) = (8, -4)$ es una solución de la ecuación $81x + 153y = 36$.

Resolvemos ahora la ecuación homogénea asociada. Es $81x + 153y = 0$, pero se simplifica en $9x + 17y = 0$. Como 9 y 17 son coprimos, su solución general es $(-17k, 9k)$.

En conclusión, la solución general de $81x + 153y = 36$ es $(x, y) = (8 - 17k, -4 + 9k)$. ♢

5
Aritmética modular

5.1 Congruencia modulo n

Los enteros se reparten entre pares e impares. Los enteros pares son los enteros cuyo resto en la división entre 2 es 0. Los impares son los restos que tienen resto 1.

En vez de repartir los enteros según su resto en la división entre 2, podemos repartirlos según su resto en la división entre 3, entre 4 ... entre cualquier entero $n \geq 2$.

Por ejemplo, hay tres restos posibles en la división entre 3, y los enteros se reparten según su resto en los tres conjuntos siguientes:

$$\{\dots, -3, 0, 3, 6, 9, \dots\}$$
$$\{\dots, -2, 1, 4, 7, 10, \dots\}$$
$$\{\dots, -1, 2, 5, 8, 11, \dots\}$$

Definicion 5.1.1. *Sea n un entero superior o igual a 2.*

Las clases de congruencia modulo n *son los conjuntos de enteros que tienen el mismo resto en la división entre n. Si a es un entero, notamos $[a]_n$ su clase de congruencia modulo n (o simplemente $[a]$ cuando n es claro por el contexto).*

Decimos que dos enteros a y b son congruentes modulo n *si pertenecen a la misma clase de congruencia modulo n, es decir, si tienen el mismo resto en la división entre n. Lo notamos: $a \equiv b \mod n$.*

Aquí está una caracterización alternativa de la congruencia.

Proposición 5.1.2. *Sea $n \geq 2$ un entero. Dos enteros a y b son congruentes modulo n si y solo si su diferencia es un múltiplo de n.*

La proposición a demostrar es de la forma $p \Leftrightarrow q$. Aquí la demostramos comprobando que si q es cierta, entonces p también, y que si p es cierta, entonces q también.

Demostración. Supongamos que $a - b$ es un múltiplo de n. Es decir, existe un entero k tal que .$a - b = kn$. Consideramos la división euclídea de b entre n: $b = qn + r$, con $0 \leq r < n$. Como $a = b + kn$, tenemos $a = (q + k)n + r$. Reconocemos en esta expresión la división euclídea de a entre n. Vemos que a tiene el mismo resto r que b en la división entre n.

Supongamos ahora que a y b son congruentes modulo n. Escribimos sus divisiones euclídeas entre n respectivas:

$$a = qn + r, \qquad b = q'n + r$$

(tienen el mismo resto ya que son congruentes). Haciendo la diferencia obtenemos $a - b = (q - q')n$. Por lo tanto $a - b$ es múltiplo de n. □

Algunos cálculos modulo 7 o 24 deben de ser familiares.

Ejemplo 5.1.1.
Si contamos 100 días a partir de hoy, ¿en qué día de la semana caerá ? Podemos resolver esta cuestión cogiendo un calendario y contando 100 días, pero un método más sencillo es utilizar el hecho de que los días de la semana se repiten en ciclos de 7. Como $100 = 14 \times 7 + 2$, dentro de 100 días será el mismo día de la semana que dentro de dos días y ésto es fácil de determinar. Aquí hemos tomado $n = 7$ y hemos reemplazado 100 por el resto de su división entre 7, es decir, por 2.

En resumen, hemos utilizado que $100 \equiv 2 \mod 7$ (100 es congruente a 2 modulo 7). ♢

Ejemplo 5.1.2.
Son las 11 de la mañana. ¿ Qué hora será dentro de 70 horas ? Tenemos $70 = 3 \times 24 - 2$. Dentro de 70 horas será la misma hora que hace dos horas: serán las 9 de la mañana. Hemos utilizado que $70 \equiv -2 \mod 24$. ♢

En regla general, si n es un entero positivo, hay n clases de congruencia modulo n, que son $[0]_n$, $[1]_n$, $[2]_n$, $\ldots$, $[n-1]_n$. La clase $[a]_n$ es exactamente el conjunto de todos los enteros de la forma $a + kn$ para $k \in \mathbb{Z}$.

Definicion 5.1.3 (Notación para el conjunto de las clases de congruencia modulo n)**.** *Sea n un entero. Notamos $\mathbb{Z}_n$ el conjunto de las clases de congruencia modulo n. Si $n > 0$,*

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$

5.2 *Aritmética (adición y multiplicación) modulo n*

Sabemos que la suma de dos enteros pares siempre es par, la suma de dos enteros impares siempre es impar, y que la suma de un entero par y de un entero impar siempre es impar. Resumimos estas leyes de la manera siguiente:

PAR + PAR = PAR
IMPAR+IMPAR=PAR
PAR+IMPAR=IMPAR

Tenemos leyes parecidas para los productos:

PAR × PAR = PAR
IMPAR × IMPAR=IMPAR
PAR × IMPAR=PAR

Podemos presentar también estas leyes por medio de tablas.

+	PAR	IMPAR
PAR	PAR	IMPAR
IMPAR	IMPAR	PAR

×	PAR	IMPAR
PAR	PAR	PAR
IMPAR	PAR	IMPAR

PAR e IMPAR son los dos elementos del conjunto $\mathbb{Z}_2$. Les habíamos notado anteriormente [0] y [1]. Las tablas anteriores con esta notación son:

Observamos que $\mathbb{Z}_2$, con esta adición y esta multiplicación, es el álgebra de Boole de dos elementos.

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

×	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

Podemos definir de manera parecida la suma y el producto de clases de congruencia modulo n para cualquier n.

Ejemplo 5.2.1.
El conjunto $\mathbb{Z}_3$ tiene tres elementos, [0], [1] y [2].

Si, por ejemplo, $x \in [0]$ e $y \in [0]$ entonces siempre se tiene $x + y \in [0]$ y $xy \in [0]$ (ver el cuadro 5.1 para convencerse con algunos ejemplos).

$x \in [0]_3$	$y \in [0]_3$	$x+y$	xy
0	0	0	0
3	0	3	0
3	3	6	9
6	0	6	0
6	3	9	18
⋮	⋮	⋮	⋮

Cuadro 5.1: Cuando $x \equiv 0 \mod 3$ e $y \equiv 0 \mod 3$ se tiene siempre $x + y \equiv 0 \mod 3$ y $xy \equiv 0 \mod 3$.

Podemos demostrarlo. Si x e y están en [0] (el conjunto de los múltiplos de 3), existen enteros i y j tal que $x = 3i$ e $y = 3j$. Entonces $x + y = 3(i + j)$ e $xy = 9ij = 3(3ij)$. Son múltiplos de 3, es decir, pertenecen a [0].

Si $x \in [1]$ e $y \in [2]$ entonces $x + y \in [0]$ y $xy \in [2]$ (ver el cuadro 5.2).

$x \in [1]_3$	$y \in [2]_3$	$x+y$	xy
1	2	3	2
4	2	6	8
4	5	9	20
7	2	9	14
7	5	12	35
⋮	⋮	⋮	⋮

Cuadro 5.2: Cuando $x \equiv 1 \mod 3$ e $y \equiv 2 \mod 3$ se tiene siempre $x + y \equiv 0 \mod 3$ y $xy \equiv 2 \mod 3$.

Lo demostramos. Como x esta en [1], existe un entero i tal que $x = 3i + 1$. Como y esta en [2], existe j tal que $y = 3j + 2$. Obtenemos: $x + y = 3i + 1 + 3j + 2 = 3i + 3j + 3$. Es un múltiplo de 3. Es decir, es un elemento de [0]. Obtenemos también $xy = (3i + 1)(3j + 2) = 9ij + 6i + 3j + 2$. Es congruente a 2 modulo 3. Es un elemento de [2].

En general, se demuestra (ver más abajo) que para cualesquiera enteros x e y, la clase modulo 3 de $x + y$ y de xy depende solamente de las clases modulo 3 de x y de y. Esto nos permite definir una adición y una multiplicación para los elementos de $\mathbb{Z}^3$ por las reglas: $[x] + [y] = [x + y]$, y $[x][y] = [xy]$. Las tablas correspondientes aparecen en el cuadro 5.3

Cuadro 5.3: Adición y multiplicación modulo 3.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

◊

Proposición 5.2.1. *Sea n en entero. Sean C_1 y C_2 dos clases modulo n.*

- *Todas las sumas de un elemento de C_1 y de un elemento de C_2 están en una misma clase modulo n. Esta clase la notamos $C_1 + C_2$, y la llamamos* suma *de las clases C_1 y C_2.*

- *Todos los productos de un elemento de C_1 y de un elemento de C_2 están también en una misma clase modulo n. Esta clase la notamos $C_1 \cdot C_2$, y la llamamos* producto de C_1 y C_2.

Demostración. Por definición de las clases de congruencia, existen enteros a y b tal que C_1 es la clase de a modulo n, y C_2 es la clase de b modulo n. Entonces los elementos de C_1 son todos los enteros de la forma $ni + a$ para $i \in \mathbb{Z}$, y C_2 es el conjunto de todos los enteros de la forma $nj + b$ para $j \in \mathbb{Z}$.

Sean x e y elementos de C_1 y C_2 respectivamente. Existen enteros i y j tal que $x = ni + a$ e $y = nj + b$. Entonces $x + y = ni + nj + a + b$, por lo tanto $x + y \in [a + b]$. Similarmente, $xy = (ni + a)(nj + b) = n^2 ij + nja + nib + ab = n(nij + ja + ib) + ab$. Por lo tanto $xy \in [ab]$. Vemos que la clase de $x + y$ siempre es la clase de $a + b$, y la clase de xy siempre es la de ab. □

Presentamos las tablas de la adición y de la multiplicación en $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$ y $\mathbb{Z}_7$ en el cuadro 5.4,

Ejemplo 5.2.2.
Calculemos el resto de la división de 28×33 entre 35, sin calcular 28×35, utilizando operaciones modulo 35 para simplificar los cálculos.

$$\left.\begin{array}{l} 28 \equiv -7 \mod 35 \\ 33 \equiv -2 \mod 35 \end{array}\right\} \quad \text{por lo tanto } 28 \times 33 \equiv (-7) \times (-2) \equiv 14 \mod 35$$

Hemos obtenido que $28 \times 33 \equiv 14 \mod 35$, es decir, que existe un entero q tal que $28 \times 33 = q \times 33 + 14$. Como, además, 14 cumple la condición: $0 \leq 14 < 35$, tiene que ser el resto en la división de 28×33 entre 35. ♢

Ejemplo 5.2.3.
Tenemos $1 \equiv 1 \mod 3$, $10 \equiv 1 \mod 3$, $100 \equiv 1 \mod 3 \ldots 10^N \equiv 1 \mod 3$ para cualquier $N \geq 0$ (se demuestra por inducción sobre N).

Por lo tanto, cualquier entero es congruente modulo 3 a la suma de los dígitos de su escritura en base 10. Por ejemplo

$$341 \equiv 3 + 4 + 1 \equiv 8 \equiv 2 \mod 3$$

Es porque $341 = 3 \times 100 + 4 \times 10 + 1 \equiv 3 \times 1 + 4 \times 1 + 1 \mod 3$.

Esto proporciona un criterio de divisibilidad por 3. Un número es divisible entre 3 si y solo si la suma de sus dígitos es congruente a 0 modulo 3.

Similarmente, tenemos que cualquier entero es congruente modulo 9 a la suma de sus dígitos. Es porque para cualquier N, el entero $10^N - 1$ es un múltiplo de 9, es $999 \cdots 9$ (N cifras). Por ejemplo $341 \equiv 3 + 4 + 1 \equiv 8 \mod 9$.

Cualquier entero es congruente modulo 11 a la suma alternada (con signos) de sus dígitos, empezando con un signo negativo para las unidades. Por ejemplo $341 \equiv -1 + 4 - 3 \equiv 0 \mod 11$ (es un múltiplo de 11). Es porque $10^N \equiv 1 \mod 11$ para N par, y $10^N \equiv -1 \mod 11$ para N impar. ♢

Cuadro 5.4: Adición y multiplicación en $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$ y $\mathbb{Z}_7$. Notamos aquí 0, 1, 2 ... en vez de [0], [1], [2] ...

Adición y multiplicación en $\mathbb{Z}_4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Adición y multiplicación en $\mathbb{Z}_5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Adición y multiplicación en $\mathbb{Z}_6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Adición y multiplicación en $\mathbb{Z}_7$:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Ejemplo 5.2.4.
¿ Es 22 051 946 un "cuadrado perfecto" (el cuadrado de un entero) ?

No, porque

$22\,051\,946 = 220\,519 \times 100 + 46 \quad \equiv 220\,519 \times 0 + 46 \mod 4 \equiv 46 \mod 4 \quad \equiv 2 \mod 4$

Si 22 051 946 fuese el cuadrado de un entero x, tendríamos que

$$22\,051\,946 \equiv x^2 \mod 4.$$

Pero cualquier entero x tiene que ser congruente a 0, 1, 2 o 3 modulo 4 y

- si $x \equiv 0 \mod 4$ entonces $x^2 \equiv 0^2 \equiv 0 \mod 4$,
- si $x \equiv 1 \mod 4$ entonces $x^2 \equiv 1^2 \equiv 1 \mod 4$,
- si $x \equiv 2 \mod 4$ entonces $x^2 \equiv 2^2 \equiv 4 \equiv 0 \mod 4$,
- y si $x \equiv 3 \mod 4$ entonces $x^2 \equiv 3^2 \equiv 9 \equiv 1 \mod 4$.

Cualquier cuadrado tiene que ser congruente a 0 o 1 modulo 4, por lo tanto 22 051 946 no es un cuadrado. ♢

Ejemplo 5.2.5.
Vamos a demostrar que para cualquier entero $n \geq 1$, el número $3^{2n+5} + 2^{4n+1}$ es divisible por 7.

Tenemos:

$$\begin{aligned} 3^{2n+5} + 2^{4n+1} &= 3^5 \cdot 3^{2n} + 2 \cdot 2^{4n} \\ &= 243 \cdot 9^n + 2 \cdot 16^n \end{aligned}$$

Trabajando módulo 7 se tiene que

$$\begin{aligned} 243 \cdot 9^n + 2 \cdot 16^n &\equiv 5 \cdot 2^n + 2 \cdot 2^n \\ &\equiv 7 \cdot 2^n \\ &\equiv 0 \end{aligned}$$

Es decir, 7 divide a $3^{2n+5} + 2^{4n+1}$ ♢

5.3 *La regla de simplificación, y los inversos y los divisores de cero en $\mathbb{Z}_n$*

Si un producto de dos enteros es 0, entonces por lo menos uno de los dos enteros tiene que ser 0. Como consecuencia, si a, b y c son enteros con $c \neq 0$, y si $ac = bc$ entonces $a = b$ (podemos "simplificar por c").

Es una consecuencia porque si $ac = bc$ entonces $(a - b)c = 0$, y se deduce que $a - b = 0$.

En los conjuntos $\mathbb{Z}_n$ las cosas son diferentes. Las dos reglas enunciadas anteriormente no siempre se cumplen.

Ejemplo 5.3.1.
En $\mathbb{Z}_6$, tenemos $[2][3] = [0]$ y sin embargo $[2] \neq [0]$ y $[3] \neq [0]$ (traducción en término de congruencias: $2 \times 3 \equiv 0 \mod 6$ pero $2 \not\equiv 0 \mod 6$ y $3 \not\equiv 0 \mod 6$) Tenemos también $[3][3] = [3][1]$ pero no podemos "simplificar por $[3]$" : $[3] \neq [1]$. O sea: $[3]a = [3]b$ no implica $a = b$ (en término de congruencias: para x e y enteros, $3x \equiv 3y \mod 6$ no implica $x \equiv y \mod 6$). ♢

Decimos que un elemento $[c]$ de $\mathbb{Z}_n$ cumple la regla de simplificación si: para cualesquiera $[a]$ y $[b]$ en $\mathbb{Z}_n$, tenemos:

"$[c][a] = [c][b]$ implica $[a] = [b]$".

Por lo tanto, $[c]$ NO cumple la regla de simplificación si y solo si existen dos elementos distintos $[a]$ y $[b]$ tal que $[c][a] = [c][b]$. Esto significa que $ca \equiv cb \mod n$. Entonces $c(a-b) \equiv 0 \mod n$, es decir, $[c][a-b] = [0] \mod n$. Como $[a] \neq [b]$ (es decir: $a \not\equiv b \mod n$), tenemos que $[a-b] \neq [0]$.

La negación de una implicación "$p \Rightarrow q$" es equivalente a la proposición "p y no q".

Esto nos proporciona una caracterización alternativa de los elementos de $\mathbb{Z}_n$ que NO cumplen la regla de simplificación.

Proposición 5.3.1. *Sea $n > 1$. Un elemento $[c]$ de $\mathbb{Z}_n$ no cumple la regla de simplificación si y solo si existe un elemento $[d]$ de $\mathbb{Z}_n$, distinto de $[0]$, tal que $[c][d] = [0]$ (existe un entero d no múltiplo de n tal que cd sea múltiplo de n).*

En este caso, y si además $[c] \neq [0]$, entonces decimos que $[c]$ es un divisor de cero *de $\mathbb{Z}_n$.*

Ejemplo 5.3.2.
En $\mathbb{Z}_6$ hay tres divisores de cero. Son $[2]$, $[3]$ y $[4]$, ya que $[2][3] = [0]$ y $[4][3] = [0]$. ♢

Demostración. Acabamos de ver que si $[c]$ no cumple la regla de simplificación entonces existe un elemento $[d] \neq [0]$ tal que (con $[d] = [a-b]$).

Recíprocamente, si $[c][d] = [0]$ con $[d] \neq [0]$, entonces $[c]$ no cumple la regla de simplificación: $[c][d] = [c][0]$ pero $[d] \neq [0]$. □

Damos también una caracterización más simple de los elementos que cumplen la regla de simplificación.

Proposición 5.3.2. *Sea $n \geq 1$. Sea $[c]$ un elemento de $\mathbb{Z}_n$. Entonces $[c]$ cumple la regla de simplificación si y solo si existe $[d]$ tal que $[c][d] = [1]$ (es decir: si y solo si existe un entero d tal que $cd \equiv 1 \mod n$). Entonces decimos que $[c]$ es una* unidad *de $\mathbb{Z}_n$, y que $[d]$ es* inverso de $[d]$.

Ejemplo 5.3.3.
Consideremos la tabla de multiplicación en $\mathbb{Z}_6$. Hay dos unidades, son $[1]$ y $[5]$. Cada una es su propia inversa, ya que $[1][1] = [1]$ y $[5][5] = [1]$.

Consideremos ahora la tabla de multiplicación en $\mathbb{Z}_7$. Todos los elementos de $\mathbb{Z}_7$, excepto $[0]$, son unidades. El inverso de $[1]$ es $[1]$, los elementos $[2]$ y $[4]$ son inversos cada uno del otro, los elementos $[3]$ y $[5]$ también, y $[6]$ es inverso de él mismo. ♢

Demostración. Suponemos que existe $[d]$ tal que $[c][d] = [1]$, y que

$$[c][a] = [c][b].$$

Multiplicamos por $[d]$ ambos lados de la ecuación:

$$[d][c][a] = [d][c][b].$$

Sustituimos $[d][c]$ por $[1]$, obtenemos

$$[1][a] = [1][b].$$

Es equivalente a $1 \times a \equiv 1 \times b \mod n$, es decir $[a] = [b]$.

Suponemos ahora que no existe ningún $[d]$ tal que $[c][d] = [1]$. Sea

$$A = \mathbb{Z}_n \setminus \{[1]\}$$

(el conjunto de los elementos de $\mathbb{Z}_n$ diferentes de $[1]$). Tiene $n-1$ elementos (ya que $\mathbb{Z}_n$ tiene n elementos y que obtenemos A quitando uno de ellos). Consideramos la aplicación "multiplicación por $[c]$" de $\mathbb{Z}_n$ en A. Es la aplicación f de $\mathbb{Z}_n$ en A que cumple: $f([x]) = [c][x]$. Como A tiene menos elementos que $\mathbb{Z}_n$, deben existir, por el principio del palomar, dos elementos distintos $[a]$ y $[b]$ tal que $f([a]) \neq f([b])$, es decir: $[c][a] \neq [c][b]$. Por lo tanto, $[c]$ no cumple la regla de simplificación. □

Las palomas son $[0], [1], [2], \ldots, [n-1]$ y los nichos son $[0], [2], [3], \ldots, [n-1]$.

Por lo tanto, para $n > 1$, los elementos de $\mathbb{Z}_n$ se reparten en tres categorías:

- El $[0]$, que va solo.
- Los divisores de cero.
- Las unidades.

Ejemplo 5.3.4.
En $\mathbb{Z}_6$ el reparto es el siguiente:

- El $[0]$, que va solo.
- Los divisores de cero son $[2]$, $[3]$ y $[4]$.
- Las unidades son $[1]$ y $[5]$.

En $\mathbb{Z}_7$ tenemos:

- El $[0]$, que va solo.
- Las unidades son todos los otros elementos:$[1], [2], \ldots, [6]$.
- No hay ningún divisor de cero.

◊

Ahora caracterizamos"sin módulos" las unidades.

Sean a y n enteros. Cada una de las proposiciones siguientes es equivalente a la anterior:

"$[a]$ es una unidad de $\mathbb{Z}_n$"
"Existe un entero u tal que $[a][u] = [1]$ en $\mathbb{Z}_n$"
"Existe un entero u tal que $au \equiv 1 \mod n$"
"Existen enteros u y v tal que $au + vn = 1$" (¡ Es una identidad de Bézout para a y n !)
"a y n son coprimos".

Acabamos de demostrar un teorema.

Teorema 5.3.3. *Sean a y n dos enteros, con $n > 0$. Entonces $[a]$ es una unidad modulo n si y solo si a y n son coprimos. En este caso, si u y v son tal que $au + nv = 1$ (identidad de Bézout para a y n) entonces $[u]$ es inverso de $[a]$ en $\mathbb{Z}_n$.*

Si a y n no son coprimos, entonces o bien $[a] = [0]$ (cuando a es un múltiplo de n), o bien $[a]$ es un divisor de cero.

El teorema anterior nos proporciona, además, un método para calcular el inverso de una unidad $[a]$ de $\mathbb{Z}_n$: calculamos una identidad de Bézout $au + vn = 1$ por medio del algoritmo de Euclides extendido. Entonces $[u]$ es inverso de $[a]$.

Ejemplo 5.3.5.
En $\mathbb{Z}_{212}$, la clase $[23]$ es una unidad, porque 23 y 212 son coprimos (porque 23 es primo pero no divide 212). Buscamos su inverso. Para esto aplicamos el algoritmo de Euclides extendido a $n = 212$ y $a = 23$.

División	Aislar el nuevo resto	Sustituir	Simplificar
$212 = 9 \times 23 + 5$	$5 = 212 - 9 \times 23$	$= n - 9\,a$	
$23 = 4 \times 5 + 3$	$3 = 23 - 4 \times 5$	$= a - 4(n - 9a)$	$= -4n + 37a$
$5 = 1 \times 3 + 2$	$2 = 5 - 3$	$= (n - 9a) - (-4n + 37a)$	$= 5n - 46a$
$3 = 1 \times 2 + 1$	$1 = 3 - 2$	$= (-4n + 37a) - (5n - 46a)$	$= -9n + 83a$
$2 = 2 \times 1 + 0$			

Hemos obtenido la identidad de Bézout

$$1 = -9n + 83a$$

De ella deducimos

$$1 \equiv 83a \equiv 83 \times 23 \mod 212$$

En consecuencia, en $\mathbb{Z}_{212}$,

$$[1] = [83][23]$$

El inverso de $[23]$ es $[83]$, la clase de 83.

Observamos que en esta identidad de Bézout para $a = 23$ y $n = 212$, el valor del coeficiente de n no sirve. Habríamos podido ahorrar unos cálculos en el algoritmo de Euclides extendido.

División	Aislar el nuevo resto	Sustituir	Simplificar
$212 = 9 \times 23 + 5$	$5 = 212 - 9 \times 23$	$= n - 9\,a \equiv -9a \mod n$	
$23 = 4 \times 5 + 3$	$3 = 23 - 4 \times 5$	$\equiv a - 4(-9a)$	$\equiv 37a \mod n$
$5 = 1 \times 3 + 2$	$2 = 5 - 3$	$\equiv (-9a) - 37a$	$\equiv -46a \mod n$
$3 = 1 \times 2 + 1$	$1 = 3 - 2$	$\equiv 37a - (-46a)$	$\equiv 83a \mod n$
$2 = 2 \times 1 + 0$			

◊

5.4 *Sistemas de ecuaciones lineales modulares (de una variable)*

En esta sección explicamos como resolver los “sistemas de ecuaciones lineales modulares de una variable” como, por ejemplo, el

siguiente:

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ 2x \equiv 1 \mod 5 \\ 3x \equiv 4 \mod 7 \end{cases} \tag{5.1}$$

Es decir, son sistemas de ecuaciones de la forma: $a_i x \equiv b_i \mod n_i$.

Como siempre, las preguntas fundamentales cuando pretendemos resolver ecuaciones son:

- ¿ Admite soluciones ?
- Si admite soluciones, ¿ Qué forma tiene el conjunto de las soluciones ? (infinito, ...)
- Describir más explícitamente el conjunto de las soluciones ("resolver el sistema")

Ejemplo 5.4.1.
El sistema (5.4) tiene como conjunto de soluciones el conjunto de los enteros de la forma $83 + 210k$ para $k \in \mathbb{Z}$. Este conjunto es mejor descrito como "la clase de 83 modulo 210". Es decir, como el conjunto de los enteros x que cumplen $x \equiv 83 \mod 210$. ♢

El resultado siguiente describe las posibles formas del conjunto de las soluciones de un sistema de ecuaciones modulares lineales.

Proposición 5.4.1. *El conjunto de las soluciones de un sistema de ecuaciones lineales modulares de una variable es o bien vacío, o bien una clase de congruencia modulo un entero.*

Ejemplo 5.4.2.
Es fácil dar ejemplos de sistemas de ecuaciones modulares lineales sin soluciones. El sistema siguiente obviamente no tiene soluciones:

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 3 \end{cases}$$

(las dos ecuaciones son incompatibles).

La ecuación $2x \equiv 1 \mod 4$ tampoco tiene ninguna solución, porque los números congruentes a 1 modulo 4 son todos impares.

No es siempre tan obvio detectar que un sistema de ecuaciones modulares lineales no tiene soluciones. El sistema siguiente no tiene soluciones, pero uno probablemente no se da cuenta de esto de inmediato.

$$\begin{cases} x \equiv 86 \mod 911 \\ x \equiv 733 \mod 799 \end{cases}$$

♢

En primer lugar explicaremos como resolvemos una única ecuación de la forma $ax \equiv b \mod n$. Será un paso de la resolución de los sistemas en general.

5.4.1 *La ecuación $ax \equiv b \mod n$*

Queremos insistir sobre dos "traducciones" importantes de la ecuación $ax \equiv b \mod n$.

- La ecuación "$ax \equiv b \mod n$" es equivalente a "$[a]_n[x]_n = [b]_n$" (por definición de las clases de congruencia y de su producto).
- La ecuación "$ax \equiv b \mod n$" es equivalente a: "existe un entero k tal que $ax + bk = n$".

Para explicar como resolver $ax \equiv b \mod n$, consideramos en primer lugar el caso cuando a es coprimo con n, es decir, cuando $[a]$ es una unidad de $\mathbb{Z}_n$. En este caso $[a]$ admite un inverso $[u]$, que calculamos por medio del algoritmo de Euclides extendido (o que encontramos por examen exhaustivo, si n es pequeño). Resolvemos la ecuación multiplicando ambos miembros de la ecuación por u. En efecto,

CASO a Y n COPRIMOS.

$$ax \equiv b \mod n$$

es equivalente a

$$[a]_n[x]_n = [b]_n$$

Es equivalente a:

$$[x]_n = [u]_n[b]_n$$

Es equivalente a

$$x \equiv ub \mod n.$$

Ejemplo 5.4.3.
Consideremos la ecuación $4x \equiv 13 \mod 47$. Como 4 es coprimo con 47, es una unidad modulo 47. Buscamos su inverso (cualquier u que cumple $4u \equiv 1 \mod 13$). Podríamos hacerlo por medio del algoritmo de Euclides extendido, pero aquí es más rápido darse cuenta que $4 \times 12 = 48 \equiv 1 \mod 47$. Por lo tanto 12 es el inverso de 4 modulo 47. Multiplicamos la ecuación por 12 y obtenemos la ecuación equivalente:

Cuando decimos que 4 es una unidad modulo 7, queremos decir que la $[4]_{47}$ (la clase de congruencia de 4 modulo 47) es una unidad de $\mathbb{Z}_{47}$.

$$48x \equiv 156 \mod 47.$$

Se simplifica (reduciendo 48 en 1 y 156 en 15) en

$$x \equiv 15 \mod 47.$$

El conjunto de las soluciones es la clase de 15 modulo 47. ♢

Consideramos ahora el caso cuando a y n no son coprimos. Sea d su Mcd. La proposición:

CASO a Y n NO COPRIMOS.

"La ecuación $ax \equiv b \mod n$ admite soluciones"

es equivalente a:

Existen enteros x y k tal que la ecuación $ax + nk = b$."

Ya sabemos que esto se cumple si y solo si $d = \text{Mcd}(a, n)$ divide b. En este caso, siempre podemos simplificar la ecuación para transformarla en una ecuación de la forma $a'x \equiv b' \mod n'$ donde a' y n' son coprimos, es decir, $[a']$ es una unidad de $\mathbb{Z}_{n'}$. Se hace así: sean $a' = a/d$, $b' = b/d$, $n' = n/d$. Entonces la ecuación

$ax \equiv b \mod n$

es equivalente a

"Existe un entero k tal que $ax + nk = b$."

Simplificando entre d, vemos que es equivalente a:

"Existe un entero k tal que $a'x + n'k = b'$."

Es equivalente a:

$a'x \equiv b' \mod n'$

Ejemplo 5.4.4.
Consideramos la ecuación

$$12x \equiv 7 \mod 15$$

Vemos que 12 no es coprimo con 15, ya que el Mcd de 12 y 15 es 3. La ecuación es equivalente a:

"Existe un entero k tal que $12x + 15k = 7$."

Como $\text{Mcd}(12, 15)$ no divide 7 no hay solución para esta ecuación diofántica. Por lo tanto, la ecuación modular tampoco tiene ninguna solución. $\Diamond$

Ejemplo 5.4.5.
Consideramos ahora la ecuación:

$$12x \equiv 6 \mod 15$$

La ecuación es equivalente a:

"Existe un entero k tal que $12x + 15k = 6$."

Simplificando entre 3, vemos que es equivalente a:

"Existe un entero k tal que $4x + 5k = 2$."

Esto es equivalente a:

$$4x \equiv 2 \mod 5$$

Como 4 es coprimo con 5, es una unidad modulo 5 (es decir la clase $[4]_5$ es una unidad de $\mathbb{Z}_5$). Como $4 \equiv -1 \mod 5$ y $(-1) \times (-1) \equiv 1 \mod 5$, vemos que $[4]_5 = [-1]_5$ es su propio inverso en $\mathbb{Z}_5$. Multiplicando por 4 la ecuación obtenemos la ecuación equivalente:

$$16x \equiv 8 \mod 5$$

que se simplifica (reduciendo 16 en 1 y 8 en 3) en

$$x \equiv 3 \mod 5.$$

En fin, el conjunto de las soluciones es la clase de congruencia de 3 modulo 5. $\Diamond$

5.4.2 *Resolución de los sistemas de ecuaciones lineales modulares*

Para saber resolver un sistema de ecuaciones lineales modulares de cualquier tamaño, basta resolver un sistema de dos ecuaciones lineales modulares. Es porque resolver un sistema de dos ecuaciones consiste en transformarlo, cuando admite soluciones, en una ecuación lineal modular única equivalente al sistema.

Ejemplo 5.4.6.
Consideramos otra vez el sistema

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ 2x \equiv 1 \mod 5 \\ 3x \equiv 4 \mod 7 \end{cases} \tag{(5.4)}$$

Resolveremos en primer lugar el sistema de las dos primeras ecuaciones:

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \end{cases}$$

Obtendremos que es equivalente a:

$$x \equiv 5 \mod 6$$

Por lo tanto el sistema inicial es equivalente a:

$$\begin{cases} x \equiv 5 \mod 6 \\ 2x \equiv 1 \mod 5 \\ 3x \equiv 4 \mod 7 \end{cases}$$

Resolveremos luego el sistema de las dos primeras ecuaciones de este nuevo sistema. Es

$$\begin{cases} x \equiv 5 \mod 6 \\ 2x \equiv 1 \mod 5 \end{cases}$$

Obtendremos que es equivalente a $x \equiv 23 \mod 30$. Por lo tanto el sistema inicial es equivalente a:

$$\begin{cases} x \equiv 23 \mod 30 \\ 3x \equiv 4 \mod 7 \end{cases}$$

Resolveremos finalmente este sistema y obtendremos que es equivalente a $x \equiv 83 \mod 210$. El conjunto de las soluciones del sistema inicial es, por lo tanto, la clase de 83 modulo 210. ♢

Aquí esta una receta para resolver un sistema de dos ecuaciones lineales modulares:

$$\begin{cases} a_1 x \equiv b_1 \mod n_1 \\ a_2 x \equiv b_2 \mod n_2 \end{cases}$$

Es conveniente, en primer lugar, resolver la primera de las ecuaciones (o alguna de las dos). Si no tiene solución, entonces el sistema tampoco tiene solución. Si tiene soluciones, esto transformo el sistema en un sistema equivalente de la forma

$$\begin{cases} x \equiv b'_1 \mod n'_1 \\ a_2 x \equiv b_2 \mod n_2 \end{cases}$$

Para resolverlo, traducimos la primera ecuación "sin módulos". Esto transforma el sistema en la formula

"Existe un entero k tal que $\begin{cases} x = b'_1 + kn'_1 \\ a_2 x \equiv b_2 \mod n_2 \end{cases}$."

Resolvemos la segunda ecuación en función de la variable k. Es decir, observamos que si $x = b'_1 + kn'_1$ entonces la segunda ecuación es equivalente a $a_2(b'_1 + kn'_1) \equiv b_2 \mod n_2$. Esta ecuación se pone en forma: $a'_2 k \equiv b'' \mod n_2$. La resolvemos. Obtenemos o bien que no tiene solución (en este caso el sistema no tiene solución) o bien que es equivalente a una ecuación de la forma $k \equiv c \mod n_2$. Esto es equivalente a:

Existe i tal que $k = c + n_2 i$

Por lo tanto, el sistema de dos ecuaciones original es equivalente a:

"Existen enteros i y k tal que $\begin{cases} x = b'_1 + (c + in_2)n'_1 \\ k = c + in_2 \end{cases}$."

Es equivalente a:

"Existe un entero i tal que $\{ x = b'_1 + (c + in_2)n'_1$"

(ya que esto basta para asegurar la existencia de un entero k tal que $k = c + in_2$). Finalmente, es equivalente a:

$$\{ x \equiv b'_1 + cn'_1 \mod n'_1 n_2$$

Ejemplo 5.4.7.
Resolvemos el sistema

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ 2x \equiv 1 \mod 5 \\ 3x \equiv 4 \mod 7 \end{cases}$$

Resolvemos en primer lugar el sistema de las dos primeras ecuaciones:

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \end{cases} \tag{5.2}$$

La primera ecuación es equivalente a: "Existe k tal que $x = 1 + 2k$". Si $x = 1 + 2k$, entonces la segunda ecuación es equivalente a $1 + 2k \equiv 2 \mod 3$. Es equivalente a $2k \equiv 1 \mod 3$. Multiplicando por el inverso de 2 modulo 3 (es 2) obtenemos la ecuación equivalente: $k \equiv 2 \mod 3$. Es equivalente a: "Existe i tal que $k = 2i + 3$". Por lo tanto, el sistema (5.2) es equivalente a

"Existen enteros i y k tal que $\begin{cases} x = 1 + 2(2 + 3i) \\ k = 2i + 3 \end{cases}$."

Es equivalente a: "Existe i tal que $x = 1 + 2(2 + 3i) = 5 + 6i$" (ya que la existencia de k es una consecuencia de esto). Es equivalente a: $x \equiv 5 \mod 6$.

Por lo tanto, el sistema inicial es equivalente a:

$$\begin{cases} x \equiv 5 \mod 6 \\ 2x \equiv 1 \mod 5 \\ 3x \equiv 4 \mod 7 \end{cases}$$

Resolvemos ahora el sistema de las dos primeras ecuaciones de este nuevo sistema. Es

$$\begin{cases} x \equiv 5 \mod 6 \\ 2x \equiv 1 \mod 5 \end{cases} \tag{5.3}$$

La primera ecuación es equivalente a: "Existe k tal que $x = 5 + 6k$". Cuando $x = 5+6k$, la segunda ecuación es equivalente a: $2(5+6k) \equiv 1 \mod 5$. Se simplifica en: $2k \equiv 1 \mod 5$. Multiplicamos por el inverso de 2 modulo 5 (vale 3) y obtenemos la ecuación equivalente: $k \equiv 3 \mod 5$. Es equivalente a: "Existe i tal que $k = 3 + 5i$". Por lo tanto el sistema (5.3) es equivalente a:

$$\text{“Existen enteros } i \text{ y } k \text{ tal que } \begin{cases} x = 5 + 6(3 + 5i) \\ k = 3 + 5i \end{cases} \text{.”}$$

Es equivalente a: "Existe i tal que $x = 5 + 6(3 + 5i) = 23 + 30i$ (ya que la existencia de k es una consecuencia). Finalmente, la solución de (5.3) es: $x \equiv 23 \mod 30$. Por tanto, el sistema original es equivalente a:

$$\begin{cases} x \equiv 23 \mod 30 \\ 3x \equiv 4 \mod 7 \end{cases} \tag{5.4}$$

La primera ecuación es equivalente a: "Existe k tal que $x = 23 + 30k$". Cuando $x = 23 + 30k$, la segunda ecuación es equivalente a: $3(23 + 30k) \equiv 4 \mod 7$. Se simplifica en: $6k \equiv 5 \mod 7$. Resolvemos esta ecuación en k. Multiplicamos por el inverso de 6 modulo 7 (es 6) y obtenemos la ecuación equivalente $k \equiv 30 \equiv 2 \mod 7$. es equivalente a: "Existe i tal que $k = 2 + 7i$", Por tanto, el sistema (5.4) es equivalente a:

$$\text{“Existen enteros } i \text{ y } k \text{ tal que } \begin{cases} x = 23 + 30(2 + 7i) \\ k = 2 + 7i \end{cases} \text{”}$$

Es equivalente a: "Existe i tal que $x = 23 + 30(2 + 7i) = 83 + 210i$ (ya que la existencia de k es una consecuencia). Esto es equivalente a: $x \equiv 83 \mod 210$.

En conclusión, el conjunto de las soluciones del sistema es la clase de 83 modulo 210. ♢

5.4.3 *El teorema chino de los restos*

El teorema siguiente da más precisiones sobre la forma del conjunto de las soluciones de un sistema de ecuaciones modulares lineales.

Teorema 5.4.2. *Sea un sistema de ecuaciones modulares lineales de la forma siguiente:*

$$\begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \\ \vdots \\ x \equiv b_r \mod n_r \end{cases}$$

Si son módulos n_1, n_2, $\ldots n_r$ son mutuamente coprimos (es decir: para cada par $i \neq j$ los módulos n_i y n_j son coprimos) entonces el conjunto de las soluciones del sistema es una clase de congruencia modulo el producto $n_1 n_2 \cdots n_r$ de los módulos.

Si no se cumple esta condición, entonces el conjunto de las soluciones del sistema es o bien vacío, o bien una clase de congruencia modulo el mínimo común múltiplo de los módulos.

Ejemplo 5.4.8.
Consideramos otra vez el sistema

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ 2x \equiv 1 \mod 5 \\ 3x \equiv 4 \mod 7 \end{cases}$$

No es de la forma considerada en el teorema. Lo ponemos de esta forma resolviendo la tercera y la cuarta ecuación: $2x \equiv 1 \mod 5$ es equivalente a $x \equiv 3 \mod 5$ y $3x \equiv 4 \mod 7$ es equivalente a $x \equiv 6 \mod 7$.

Por tanto, el sistema es equivalente a:

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 6 \mod 7 \end{cases}$$

Comprobamos ahora que los módulos son mutuamente coprimos: 2 y 3 son coprimos, 2 y 5 son coprimos, 2 y 7 son coprimos, 3 y 5 son coprimos, 3 y 7 son coprimos, 5 y 7 son coprimos. El teorema chino de los restos asegura que la solución del sistema es una clase de congruencia modulo $2 \times 3 \times 5 \times 7 = 210$. ♢

Ejemplo 5.4.9.
Consideramos el sistema

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \end{cases}$$

Como 2 y 3 son coprimos, el teorema chino de los restos asegura que el conjunto de las soluciones del sistema es una clase de congruencia modulo 6. Podemos examinar todos los casos posibles: ver el cuadro 5.5. Obtenemos como solución: $x \equiv 5 \mod 6$.

x	0	1	2	3	4	5
$x \mod 2$	0	1	0	1	0	1
$x \mod 3$	0	1	2	0	1	2

Cuadro 5.5: Clases de congruencia modulo 2 y 3 de los enteros del 0 al 5.

♢

El teorema chino de los restos tiene la consecuencia importante siguiente. Sea n un entero, producto de números mutuamente coprimos $n_1, n_2, \ldots, n_r$. Entonces la clase modulo n_1 de cualquier entero x depende solamente de su clase modulo n. Es porque si los números en una misma clase modulo n se obtienen cada uno de cada otro añadiendo un múltiplo de n. Pero los múltiplos de n son también múltiplos de n_1, y por lo tanto los números están también en la misma clase modulo n_1.

Ejemplo 5.4.10.
La clase modulo 3 de un entero x depende solamente de su clase modulo 6: si $x \equiv 0 \mod 6$ entonces $x \equiv 0 \mod 3$, si $x \equiv 1 \mod 6$ entonces $x \equiv 1 \mod 3, \ldots$, si $x \equiv 5 \mod 6$ entonces $x \equiv 2 \mod 3$. $\Diamond$

Similarmente, las clases modulo $n_2, \ldots, n_r$ de cualquier entero están determinadas por su clase modulo n. Tenemos por lo tanto una aplicación f que asocia a cada clase modulo n la sucesión de sus clases modulo $n_1, n_2, \ldots, n_r$. Su conjunto de salida es $\mathbb{Z}_n$, y su conjunto de llegada es el conjunto de sucesiones

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_r}.$$

En formulas, $f([x]_n) = ([x]_{n_1}, [x]_{n_2}, \ldots, [x]_{n_r})$.

Ejemplo 5.4.11.
Aquí esta un ejemplo explicita, con $n = 30$ y $n_1 = 2$, $n_2 = 3$ y $n_3 = 5$. La aplicación f es la aplicación de $\mathbb{Z}_{30}$ en $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ definida por:

$$f([x]_{30}) = ([x]_2, [x]_3, [x]_5).$$

Por ejemplo, $f([14]_{30}) = ([0]_2, [2]_3, [4]_5)$ porque para cualquier entero x congruente a 14 modulo 30 se tiene $x \equiv 0 \mod 2$, $x \equiv 2 \mod 3$ y $x \equiv 4 \mod 5$.

Cuadro 5.6: La aplicación f que asocia a cada clase modulo 30 sus clases modulo 2, 3 y 5.

$0 \mapsto (0,0,0)$	$10 \mapsto (0,1,0)$	$20 \mapsto (0,2,0)$
$1 \mapsto (1,1,1)$	$11 \mapsto (1,2,1)$	$21 \mapsto (1,0,1)$
$2 \mapsto (0,2,2)$	$12 \mapsto (0,0,2)$	$22 \mapsto (0,1,2)$
$3 \mapsto (1,0,3)$	$13 \mapsto (1,1,3)$	$23 \mapsto (1,2,3)$
$4 \mapsto (0,1,4)$	$14 \mapsto (0,2,4)$	$24 \mapsto (0,0,4)$
$5 \mapsto (1,2,0)$	$15 \mapsto (1,0,0)$	$25 \mapsto (1,1,0)$
$6 \mapsto (0,0,1)$	$16 \mapsto (0,1,1)$	$26 \mapsto (0,2,1)$
$7 \mapsto (1,1,2)$	$17 \mapsto (1,2,2)$	$27 \mapsto (1,0,2)$
$8 \mapsto (0,2,3)$	$18 \mapsto (0,0,3)$	$28 \mapsto (0,1,3)$
$9 \mapsto (1,0,4)$	$19 \mapsto (1,1,4)$	$29 \mapsto (1,2,4)$

Observamos que esta aplicación es biyectiva: cada elemento del conjunto de llegada es imagen de exactamente un elemento de $\mathbb{Z}_{30}$ (se ve porque cada elemento del conjunto de llegada aparece exactamente una vez en el cuadro 5.6).

Determinar el antecedente de un elemento $([b_1]_2, [b_2]_3, [b_3]_5)$ es determinar la clase $[x]_{30}$ tal que $f([x]_{30}) = ([b_1]_2, [b_2]_3, [b_3]_5)$. Es decir, es determinar los enteros x que cumplen:

$$\begin{cases} x \equiv b_1 \mod 2 \\ x \equiv b_2 \mod 3 \\ x \equiv b_3 \mod 5 \end{cases}$$

$\Diamond$

Determinar los antecedentes de un elemento $([b_1]_{n_1}, [b_2]_{n_2}, \dots, [b_r]_{n_r})$, es resolver el sistema:

$$\begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \\ \vdots \\ x \equiv b_r \mod n_r \end{cases}$$

El teorema chino de los restos asegura que el conjunto de las soluciones de este sistema es una clase modulo n ¡ Significa que

$$([b_1]_{n_1}, [b_2]_{n_2}, \dots, [b_r]_{n_r})$$

siempre tiene un único antecedente ! O sea, que la aplicación f es biyectiva.

Como es más fácil calcular los enteros n_1, n_2 ... (más pequeños) que modulo n (más grande), esta aplicación f se utiliza a veces para simplificar cálculos.

Ejemplo 5.4.12.
Digamos que queremos calcular $2^{2\,000}$ modulo 5040. El modulo $n = 5040$ se descompone en primos como $2^4 \times 3^2 \times 5 \times 7$. Ponemos $n = 5040$ y $n_1 = 2^4 = 16$, $n_2 = 3^2 = 9$, $n_3 = 5$ y $n_4 = 7$. Son mutuamente coprimos. Consideramos la aplicación f que asocia a cada clase $[x]_{5040}$ la sucesión $([x]_{16}, [x]_9, [x]_5, [x]_7)$. Es una biyección. Calculamos la imagen de $[2^{2000}]_{5040}$, es decir, calculamos $[2^{2000}]_{16}$, $[2^{2000}]_9$, $[2^{2000}]_5$ y $[2^{2000}]_7$.

Observamos que $2^4 = 16 \equiv 0 \mod 16$. Por lo tanto

$$2^{2000} = (2^4)^{500} \equiv 0^{500} \equiv 0 \mod 16.$$

Por tanto, $[2^{2000}]_{16} = [0]_{16}$.

Luego observamos que $2^3 = 8 \equiv -1 \mod 9$. Por lo tanto $2^6 = (2^3)^2 \equiv (-1)^2 \equiv 1 \mod 9$. Pero tendremos también $2^{12} \equiv 1 \mod 9$, $2^{18} \equiv 1 \mod 9$ .... Hacemos la división euclídea de 2000 entre 6: $2000 = 6 \times 333 + 2$. Por lo tanto,

$$2^{2000} = (2^6)^{333} \times 2^2 \equiv 1^{333} \times 2^2 \equiv 4 \mod 6.$$

En conclusión, $[2^{2000}]_9 = [4]_9$.

Similarmente, calculamos que $[2^{2000}]_5 = [1]_5$ (con el pequeño teorema de Fermat) y que $[2^{2000}]_7 = [4]_7$.

Hemos obtenido que

$$f([2^{2000}]_{5040}) = ([0]_{16}, [4]_9, [1]_5, [4]_7).$$

Por tanto, $[2^{2000}]_{5040}$ es la clase–solución del sistema:

$$\begin{cases} x \equiv 0 \mod 16 \\ x \equiv 4 \mod 9 \\ x \equiv 1 \mod 5 \\ x \equiv 4 \mod 7 \end{cases}$$

Se resuelve el sistema y se obtiene como solución: $x \equiv 256 \mod 5040$.
En conclusión,

$$2^{2000} \equiv 256 \mod 5040.$$

◊

5.5 *Las potencias de una unidad*

Ejemplo 5.5.1.
Consideramos (cuadro 5.8) las potencias sucesivas de los elementos no nulos de, digamos, $\mathbb{Z}_7$ (para considerar un ejemplo).

Cuadro 5.7: Potencias de los elementos no nulos de $\mathbb{Z}_p$.

a	a^2	a^3	a^4	a^5	a^6	a^7	$\ldots$
1	1	1	1	1	1	1	
2	4	1	2	4	1	2	
3	2	6	4	5	1	3	
4	2	1	4	2	1	4	
5	4	6	2	3	1	5	
6	1	6	1	6	1	6	

Observamos:

- que cada unidad tiene una potencia igual a $[1]$.
- y, además, que para todas las unidades se tiene $a^6 = [1]$.

Las mismas observaciones se repiten en todos los $\mathbb{Z}_p$ con p primo: todos los elementos no nulos a la potencia $p-1$ dan $[1]$. $\Diamond$

Teorema 5.5.1 (Pequeño teorema de Fermat). *Sea p un número primo. Si a no es un múltiplo de p entonces $a^{p-1} \equiv 1 \mod p$.*

El "gran" teorema de Fermat es el teorema que fue demostrado hace solamente unos años (mientras que fue enunciado por Fermat al siglo XXVII): que la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras cuándo $n \geq 3$.

Para la demostración utilizaremos la aplicación "multiplicación por $[a]$" de $\mathbb{Z}_p \setminus \{[0]\}$ en $\mathbb{Z}_p \setminus \{[0]\}$.

Recordamos que "a no es múltiplo de p" es equivalente a: "la clase de a modulo p no es $[0]$", y que "$a^{p-1} \equiv 1 \mod p$" es equivalente a "$[a]^{p-1} = [1]$".

Ejemplo 5.5.2.
Presentamos en un caso particular lo que será la demostración general. Consideramos el caso $p = 7$ y $a = 2$. La aplicación "multiplicación por $[2]$" de $\mathbb{Z}_7 \setminus \{[0]\}$ en $\mathbb{Z}_7 \setminus \{[0]\}$ viene dada por:

$$[1] \longmapsto [1] \times [2] = [2]$$
$$[2] \longmapsto [2] \times [2] = [4]$$
$$[3] \longmapsto [3] \times [2] = [6]$$
$$[4] \longmapsto [4] \times [2] = [1]$$
$$[5] \longmapsto [5] \times [2] = [3]$$
$$[6] \longmapsto [6] \times [2] = [5]$$

Tenemos por lo tanto:

$$([1] \times [2]) \times ([2] \times [2]) \times ([3] \times [2]) \times ([4] \times [2]) \times ([5] \times [2]) \times ([6] \times [2]) \\ = [1] \times [2] \times [3] \times [4] \times [5] \times [6]$$

Como $[1]$, $[2]$, $\ldots$, $[6]$ son unidades y aparecen en ambos lados, podemos simplificar por ellos. Obtenemos:

$$[2]^6 = [1]$$

$\Diamond$

Demostración. Como a no es múltiplo de p y p es primo, $[a]$ es una unidad de $\mathbb{Z}_p$. Si $[b]$ es cualquier elemento de $\mathbb{Z}_p$ distinto de $[0]$, entonces $[b] \times [a]$ todavía es distinto de 0 (sino $[a]$ sería un divisor de cero o $[0]$, pero no es el caso, ya que es una unidad).

Por lo tanto, hay una aplicación "multiplicación por $[a]$", que va de $\mathbb{Z}_p \setminus \{[0]\}$ en $\mathbb{Z}_p \setminus \{[0]\}$. Esta aplicación es biyectiva. Es porque los antecedentes de un elemento $[b]$ de $\mathbb{Z}_p \setminus \{[0]\}$ es una solución x de la ecuación:

$$[b] = x[a]$$

Como $[a]$ es una unidad, tiene un inverso $[a']$. La ecuación es equivalente a :

$$[a'][b] = x$$

Vemos por lo tanto que tiene una, y solamente una solución. Es decir, $[b]$ siempre tiene un único antecedente. Por definición, significa que la aplicación es biyectiva.

Como consecuencia, los elementos:

$$[1] \times [a], [2] \times [a], [3] \times [a], \ldots, [p-1] \times [a]$$

son exactamente todos los elementos de $\mathbb{Z}_p \setminus \{[0]\}$, quizás en un orden diferente. En todo caso, el producto de todos estos elementos es igual al producto de todos los elementos de $\mathbb{Z}_p \setminus \{[0]\}$, es decir:

$$[1] \times [a] \times [2] \times [a] \times [3] \times [a] \times \cdots \times [p-1] \times [a] = \\ [1] \times [2] \times [3] \times \cdots \times [p-1]$$

Como $[1]$, $[2]$, $[3]$, ... son todos unidades, podemos simplificar. Obtenemos:

$$[a]^{p-1} = [1]$$

□

La demostración anterior se generaliza al caso no primo: en vez de considerar todos los elementos no nulos de $\mathbb{Z}_n$, consideramos solamente las unidades. Obtenemos el resultado siguiente.

Teorema 5.5.2 (Teorema de Euler). *Sea n un entero positivo y sea $\phi(n)$ el número de unidades en $\mathbb{Z}_n$. Sea a un entero coprimo con n. Entonces:*

$$a^{\phi(n)} \equiv 1 \mod n$$

Demostración. En primer lugar, observamos que $[a]$ es una unidad de $\mathbb{Z}_n$ (ya que a es coprimo con n).

Sea U el conjunto de las unidades de $\mathbb{Z}_n$. Si $[b]$ es una unidad, entonces $[b] \times [a]$ también es una unidad. En efecto, como $[a]$ y $[b]$ son unidades, tienen inversos $[a']$ y $[b']$. Tenemos:

$$\begin{aligned} [b] \times [a] \times [a'] \times [b'] &= [b] \times [1] \times [b'] && \text{ya que } [a'] \text{ es inverso de } [a] \\ &= [b] \times [b'] \\ &= [1] && \text{(ya que } [b'] \text{ es inverso de } [b]\text{)} \end{aligned}$$

Vemos que $[b] \times [a]$ admite un inverso (concretamente es $[a'] \times [b']$).

Por lo tanto, hay una aplicación "multiplicación por $[a]$" que va de U en U. Es biyectiva (porque la ecuación $[b] = x[a]$ es equivalente a $[a'][b] = x$, donde $[a']$ es el inverso de $[a]$). Por lo tanto, el producto de las unidades multiplicadas por $[a]$ (cada una) es igual al producto de las unidades. Simplificando por todas las unidades deducimos que $[a]^{\phi(n)} = [1]$. □

El pequeño teorema de Fermat sirve también para elaborar tests de primalidad: ver el texto de la práctica 5.

Ejemplo 5.5.3.
Consideramos (cuadro 5.8) las potencias sucesivas de los elementos, digamos, de $\mathbb{Z}_{20}$ (para considerar un ejemplo). Son las clases de 1, 3, 7, 9, 11, 13, 17 y 19.

Cuadro 5.8: Potencias de las unidades en $\mathbb{Z}_{20}$.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1
3	9	7	1	3	9	7	1	3	9
7	9	3	1	7	9	3	1	7	9
9	1	9	1	9	1	9	1	9	1
11	1	11	1	11	1	11	1	11	1
13	9	17	1	13	9	17	1	13	9
17	9	13	1	17	9	13	1	17	9
19	1	19	1	19	1	19	1	19	1

Observamos:

- que cada unidad tiene una potencia igual a $[1]$.
- y, además, que, conformemente al teorema de Euler, para todas las unidades $[a]$ se tiene $[a]^8 = [1]$.

◊

5.6 *El número de unidades en $\mathbb{Z}_n$ (la función ϕ de Euler)*

Nos planteamos aquí el problema de contar las unidades de $\mathbb{Z}_n$.

Definicion 5.6.1. *Para cualquier entero $n \geq 2$, se suele notar $\phi(n)$ el número de unidades en $\mathbb{Z}_n$. La aplicación ϕ se llama* función ϕ de Euler.

Como los elementos de $\mathbb{Z}_n$ son exactamente las clases $[0]$, $[1]$, $[2]$, ..., $[n-1]$, y que una clase $[a]$ es una unidad si y solo si a es coprimo con n, vemos que $\phi(n)$ cuenta también los enteros k que cumplen $0 \leq k < n$ y que son coprimos con n.

Ejemplo 5.6.1.
Tenemos $\phi(12) = 4$ ya que hay 4 unidades en $\mathbb{Z}_{12}$ (son $[1]$, $[5]$, $[7]$ y $[11]$). Equivalentemente, hay 4 números coprimos con 12 en $\{0, 1, 2, \ldots, 11\}$ (son 1, 5, 7 y 11). ◊

Hay formulas para $\phi(n)$. Hay que ser capaz de obtenerlas por lo menos en los tres casos simples siguientes:

- Cuando $n = p$, un primo.
- Cuando $n = p^r$, una potencia de un primo.
- Cuando $n = pq$, el producto de dos primos distintos.

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4

Cuadro 5.9: Los primeros valores de la función ϕ de Euler.

Si p es un primo, entonces los números que no son coprimos con p son sus múltiplos. En $\{0, 1, 2, \ldots, p-1\}$ el único múltiplo de p es 0, y los coprimos con p son los otros $p-1$ elementos. Por lo tanto $\phi(p) = p - 1$.

Si n es potencia de un primo p, $n = p^r$, entonces los números que no son coprimos con n son los múltiplos de p. En $\{0, 1, 2, \ldots, p^r - 1\}$ son:

$$0, p, 2p, \ldots, p^r - 2p, p^r - p$$

Son los números de la forma kp con k en la lista:

$$0, 1, 2, \ldots, p^{r-1} - 2, p^{r-1} - 1$$

Son, por lo tanto $1 + (p^{r-1} - 1) = p^{r-1}$. En consecuencia, en $\{0, 1, 2, \ldots, p^r - 1\}$ el número de enteros coprimos con n es

$$\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1).$$

Si $n = pq$ es un producto de dos primos distintos p y q, los enteros que no son coprimos con n son los múltiplos de p y los múltiplos de q. Podemos formar los conjuntos siguientes de enteros k entre 0 y $n-1$:

- El conjunto A de los múltiplos de p. Explícitamente,

  $$A = \{0, p, 2p, \ldots, (q-1)p\}.$$

  Este conjunto A tiene q elementos.

- El conjunto B de los múltiplos de q. Explícitamente,

  $$B = \{0, q, 2q, \ldots, (p-1)q\}.$$

  Este conjunto B tiene p elementos.

Los números entre 0 y $n-1$ que no son coprimos con n son los elementos de $A \cup B$. Utilizamos la formula de inclusión–exclusión:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Los elementos de $A \cap B$ son los múltiplos comunes de p y q que están entre 0 y $n-1$. Como p y q son coprimos, su mcm es $pq = n$. Por lo tanto $A \cap B = \{0\}$, y $|A \cap B| = 1$. Obtenemos:

$$|A \cup B| = q + p - 1$$

Hay $q + p - 1$ enteros entre 0 y $n - 1$ que no son coprimos con n. El número de enteros coprimos con n entre 0 y $n - 1$ es, por lo tanto, $n - (p + q - 1)$. Como $n = pq$, este número es $pq - p - q + 1$. Se simplifica en $(p - 1)(q - 1)$.

El cuadro 5.10 recuerda las tres formulas que hemos obtenido en estos casos particulares. Estas formulas son más fáciles de recordar si, en vez de considerar el número $\phi(n)$ de unidades en $\mathbb{Z}_n$, considera,s la *proporción* $\phi(n)/n$ de unidades.

Caso	Número de unidades en $\mathbb{Z}_n$	proporción de unidades en $\mathbb{Z}_n$
$n = p$, primo	$\phi(p) = p - 1$	$\frac{\phi(n)}{n} = 1 - \frac{1}{p}$
$n = p^r$, potencia de primo	$\phi(p^r) = p^{r-1}(p - 1)$	$\frac{\phi(n)}{n} = (1 - \frac{1}{p})$
$n = pq$, producto de dos primos distintos	$\phi(pq) = (p - 1)(q - 1)$	$\frac{\phi(n)}{n} = (1 - \frac{1}{p})(1 - \frac{1}{q})$

Cuadro 5.10: Formulas para $\phi(n)$ en tres casos importantes y sencillos.

Tenemos la formula general siguiente.

Teorema 5.6.2 (Formula general para la función de Euler)**.** *Sea n un entero positivo cuyos factores primos (distintos) son $p_1, p_2, \ldots, p_r$. Entonces la proporción de unidades en $\mathbb{Z}_n$ es el producto de los números $(1 - \frac{1}{p_i})$. Es:*

$$\frac{\phi(n)}{n} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

Obsérvese que precisamente, $(1 - \frac{1}{p_i})$ es la proporción de números coprimos con p_i en $\{0, 1, 2 \ldots, n - 1\}$. El teorema de Euler asegura, por lo tanto, que para los números de $\{0, 1, \ldots, n - 1\}$, la probabilidad de ser coprimo con n es el producto de las probabilidades de ser coprimo con cada uno de sus factores primos.

Demostración. Omitida. □

Ejemplo 5.6.2.
Calculemos $\Phi(n)$ para $n = 71\,475$. La descomposición en factores primos de n es

$$3 \times 5^2 \times 953$$

En particular, sus factores primos son 3, 5 y 953. Por lo tanto, la proporción de unidades en $\mathbb{Z}_n$ es:

$$\begin{aligned}\frac{\Phi(n)}{n} &= \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\cdots\left(1 - \frac{1}{953}\right)\\ &= \frac{2}{3}\cdot\frac{4}{5}\cdot\frac{952}{953}\end{aligned}$$

Por lo tanto el número de unidades en $\mathbb{Z}_n$ es:

$$\begin{aligned}\Phi(n) &= n \cdot \frac{2}{3}\cdot\frac{4}{5}\cdot 952953\\ &= 3 \times 5^2 \times 953 \times \frac{2}{3}\cdot\frac{4}{5}\cdot 952953\\ &= 5 \times 2 \times 4 \times 952\\ &= 38\,080\end{aligned}$$

◊

5.7 La matemática del sistema criptográfico RSA

Sección todavía en fase de elaboración.